UNIVERZA NA PRIMORSKEM

FAKULTETA ZA VEDE O ZDRAVJU

MAGISTRSKA NALOGA

SAMANTA MIKULETIČ

Izola, 2016

UNIVERZA NA PRIMORSKEM

FAKULTETA ZA VEDE O ZDRAVJU

INFORMACIJSKA VARNOST NA PODROČJU ZDRAVSTVENE NEGE

INFORMATION SECURITY IN NURSING

Študent: SAMANTA MIKULETIČ

Mentor: doc. dr. BOŠTJAN ŽVANUT

Somentor: mag. TAMARA ŠTEMBERGER KOLNIK, viš. pred.

Študijski program: študijski program 2. stopnje Zdravstvena nega

Izola, 2016

IZJAVA O AVTORSTVU

Spodaj podpisana Samanta Mikuletič izjavljam, da je predložena magistrska naloga izključno rezultat mojega dela;

- sem poskrbela, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oziroma citirana v skladu s pravili UP Fakultete za vede o zdravju;
- se zavedam, da je plagiatorstvo po Zakonu o avtorskih in sorodnih pravicah UL št. 16/2007 (v nadaljevanju ZASP) kaznivo.

KLJUČNE INFORMACIJE O DELU

Naslov	Informacijska varnost na področju zdravstvene nege
Tip dela	magistrska naloga
Avtor	MIKULETIČ, Samanta
Sekundarni avtorji	ŽVANUT, Boštjan (mentor) / ŠTEMBERGER KOLNIK, Tamara (so-mentorica) / ČERNELIČ BIZJAK, Maša (recenzentka) / PUCER, Patrik (recenzent)
Institucija	Univerza na Primorskem, Fakulteta za vede o zdravju
Naslov inst.	Polje 42, 6310 Izola
Leto	2016
Strani	VII, 74 str., 2 preg., 12 sl., 3 pril., 78 virov
Ključne besede	Zdravstvena nega, informacijska varnost, varnostno vedenje, varovanje podatkov
UDK	004.056:616-083
Jezik besedila	slv
Jezik povzetkov	slv/ang

Izvleček Največja nevarnost razkritja osebnih podatkov za področje zdravstvene nege je zaposleni v zdravstvenem varstvu, ki se ne zaveda in ne ve, kako pomembna je sama zaupnost podatkov. Številne študije poročajo o neustreznem vedenju medicinskih sester, zato je njegovo poznavanje še kako pomembno. Po delu se iz informacijskega sistema vedno odjavi 82,05 % medicinskih sester, po zapustitvi delovne postaje slednjo zaklene le 36,54 %. Problematika nerazumevanja informacijske varnosti predstavlja nevarnost na področju varovanja osebnih pacientovih podatkov.

KEY WORDS DOCUMENTATION

Title	Information security in nursing
Type	Master's Thesis
Author	MIKULETIČ, Samanta
Secondary authors	ŽVANUT, Boštjan (supervisor) / ŠTEMBERGER KOLNIK, Tamara (coadvisor) / ČERNELIČ BIZJAK, Maša (reviewer) / PUCER, Patrik (reviewer)
Institution	University of Primorska Faculty of Health Sciences
address	Polje 42, 6310 Izola
Year	2016
Pages	VII, 74 p., 2 tab., 12 fig., 3 ann., 78 ref.
Keywords	Nursing, information security, security behaviours, data security
UDC	004.056:616-083
Language	slv
Abstract language	slv/eng

Abstract The greatest danger of personal data disclosure in the field of health care is the employee in health care, who is not aware and does not know the importance of the confidentiality of the data itself. Numerous studies have reported improper behaviour of the nursing staff, therefore the knowledge regarding this matter is ever so important. When finished working 82.05 % of the respondents always checkes out of the information system, but only 36.54 % of the respondents locks the computer after leaving the workstation. The problematic of misunderstanding of the information security represents a threat in the field of protection of personal patient data.

KAZALO VSEBINE

KAZALO SLIK

KAZALO PREGLEDNIC

SEZNAM KRATIC

1KA	en klik anketa (www.1ka.si)
AAA	angl. »Authentication, Authorization, Accounting« - preverjanje pristnosti, pooblaščanje, vodenje računov
AACN	angl. »American Association of Colleges in Nursing« - Ameriško združenje fakultet zdravstvene nege
EHRS	angl. »Electronic Health Records« - elektronski zdravstveni zapisi
HAIS-Q	angl. »Human Aspects of Information Security Questionnaire« - vprašalnik za prepoznavanje človeškega vidika informacijske varnosti
HTML	angl. »Hyper Text Markup Language« - jezik za označevanje hiperteksta
ID	angl. »Identity card« - osebna izkaznica
IC	angl. »Identity code« - identifikacijska koda/oznaka
IKT	Informacijsko-komunikacijska tehnologija - angl. »information and communication technology«
IOM	angl. »Institute of Medicine« - medicinski inštitut
InfoSec	angl. »information security« - informacijska varnost
IS	angl. »information system« - informacijski sistem
IT	angl. »information technology« - informacijska tehnologija
OP	osebni podatek - angl. »personal data«
PIN	angl. »Personal Identification Number« - osebna identifikacijska številka
SUIV	Sistem za upravljanje informacijske varnosti - angl. »information security management«
SSKJ	Slovar slovenskega knjižnega jezika - angl. »Dictionary of Slovenian literary language«
TIGER	angl. »The Technology Informatics Guiding Educational Reform«
UCE	angl. »Unsolicated Commerccial Email« - neželena elektronska pošta/spam OP
UISAQ	angl. »User's Information Security Awareness Questionnaire« - vprašalnik za prepoznavanje vedenja in oceno znanja informacijske varnosti
ZVOP	Zakon o varstvu osebnih podatkov (www.uradni-list.si)

1 UVOD

V današnjih dneh ni časopisa, v katerem ne bi zasledili šokantne zgodbe o kršitvi informacijske varnosti ali invaziji v zasebnost (Deloitte, 2011). Vprašanje zasebnosti je problematično in se dotika pravic vsakega posameznika. Pri tem se srečujemo s hitro razvijajočo se tehnologijo (Kovačič, 2006, str. 7). Informacijska tehnologija je postala sestavni del sodobnega življenja. Za mnoge ljudi je življenje brez spleta, elektronske pošte, spletnega nakupovanja, uporabe pametnih telefonov in spletnih bank, praktično nemogoče (Deloitte, 2011). Vlade po svetu prepoznavajo urgentno in vedno večjo potrebo po izboljšani informacijski varnosti. Dogajajo se spremembe v praksi na ravni organizacije, politike in državnih zakonov, ki zadevajo zasebnost in varnost informacij. Nastajajo novi zakoni in strožji predpisi, ki naj bi bili v pomoč pri zaščiti državljanov pred škodo (Egan in Mather, 2005; Dimitropoulos in Rizk, 2009; Deloitte, 2011). Ni naključje, da pri varstvu elektronske zasebnosti pogosto naletimo na poudarjanje zgolj tehničnega varovanja in informacijske varnosti, pomen zakonodaje in varnostne kulture pa je mnogokrat spregledan (Kovačič, 2006). Organizacije se pri vodenju poslovanja vedno bolj zanašajo na tehnologijo, tako je varnost postala velik problem. Varnostna tveganja povezana z informacijsko tehnologijo (v nadaljevanju IT), so aktualna področja, ki postajajo vedno pomembnejša (Kruger in Kearney, 2006). V IT je vključenih veliko sistemov (npr. družabne spletne strani, telefonija, elektronska pošta, sistemi sporočanja, bančništvo) (Bratuša, 2010). Informacijsko-komunikacijska tehnologija (v nadaljevanju IKT) ogroža različne oblike varnosti posameznika, družbe in institucionalnih akterjev (Svete in Pinterič, 2008). Vsakodnevno je povprečni uporabnik informacijskih sistemov (v nadaljevanju IS) podvržen tveganju vdorov, ribarjenju [1] (angl. »phishing«), kraji identitete[2], odtujitvi bančnih računov, izsiljevanju itn. (Svete in Pinterič, 2008; Bratuša, 2010). Vse do nedavnega so bila prizadevanja za zagotavljanje varnosti osredotočena zgolj na tehnologijo, dokler se ni izkazalo, da ima človeški faktor pri tem ključno vlogo (Lineberry, 2007; Trček in sod., 2007).

Številne raziskave o informacijski varnosti se osredotočajo na človeško vedenje (npr. zavedanje varovanja informacij v sklopu računalniškega kriminala in politike varovanja informacij). Namenjene so zmanjševanju groženj in prepričanju, da lahko vedenje uporabnikov vpliva na varnost IS (Kruger in Kearney, 2006). Znani pristopi za izvajanje nadzora varovanja informacij se dotikajo človekovih komponent, kot sta ozaveščanje in izobraževanje, se pa ne osredotočajo na zaposlenega ali na to, kako usmerjati, meriti in spremeniti njegovo obnašanje ali vedenje (Eloff in Eloff, 2005). Medtem ko številni dokazi povezujejo IT z izboljšano varnostjo pacientov, kakovostno zdravstveno nego, dostopom in učinkovitostjo, morajo medicinske sestre imeti potrebne kompetence za uporabo računalnika, informatike in informacijske pismenosti, tako v praksi in izobraževanju, kakor tudi v raziskovanju. Na žalost pa mnogi nimajo teh sposobnosti (Fetter, 2009a). Zaradi naglega razvoja IKT se je število ustanov, kjer medicinske sestre

[1] Uporabnik interneta aktivira povezavo (podtaknjene URL povezave, največkrat v el. pošto ali druge spletne strani), ki se izdaja za spletno stran banke. Tako lahko uporabnik pridobi številko kreditne/bančne kartice in druge pomembne podatke (Verdonik in Bratuša, 2005).

[2] Gre za prevzemanje identitete ali ponarejanje identitete, da si nekdo pridobi dostop do sistema tako, da se izdaja za pooblaščenega uporabnika. To lahko stori elektronsko, s pošiljanjem e-pošte, ki je označena kot zaupna. Sem prištevamo tudi nemarno ravnanje z uporabniškim imenom in geslom, ki ju lahko dobi nekdo s slabim namenom (Egan in Mather, 2005, str. 107).

uporabljajo računalnike za zbiranje, preverjanje, vnašanje in beleženje podatkov pacientov močno povečalo (Niimi in Ota, 2014). Pričakovanje subjektivnih in odgovornih vedenj posameznih medicinskih sester se je povečalo skupaj s spremembami v družbi. Poznavanje varnostnega vedenja medicinskih sester je pomembno za zasebnost pacientov in drugega zdravstvenega osebja (Niimi in Ota, 2014). Pomembno je, da se medicinske sestre osredotočajo na aktivno reševanje problemov, da testirajo in ocenjujejo rešitve zdravstveno-negovalnih problemov z uporabo IKT (Abbott in Coenen, 2008; Forbes in While, 2009; While in Dewsbury, 2011). Vsi našteti razlogi nakazujejo na to, da je raziskovanje omenjenega področja ključnega pomena za zdravstvo.

V nadaljevanju naloge so predstavljena teoretična izhodišča, ki zadevajo predvsem IKT in etiko na področju zdravstvene nege, informacijsko varnost in zasebnost, varovanje podatkov pred osebjem, vedenja uporabnikov, fizično zaščito, varnostno kopiranje osebnih podatkov, gesla, elektronsko pošto in varnostno politiko ter rešitve. Sledi poglavje Metode dela in materiali, kjer je opisan potek raziskave, uporabljene metode, merski instrument in vzorec. V poglavju Rezultati smo predstavili rezultate analize podatkov, ki smo jih pridobili s pomočjo spletne ankete. V Razpravi smo povzeli ključne rezultate in jih primerjali z drugimi tujimi opravljenimi raziskavami. V Zaključku so povzete ugotovitve naloge in predlogi za nadaljnje delo.

1.1 Informacijsko-komunikacijska tehnologija in etika

»IT vključuje vse tehnologije, ki se uporabljajo za zbiranje, obdelovanje, shranjevanje in zaščito podatkov. Nanaša se na računalniško strojno opremo (angl. »hardware«), programsko opremo (angl. »software«) in računalniško omrežje. Ključni atributi IT, ki omogočajo pridobivanje podatkov za podporo pacienta, rezultate in procese odločanja v zdravstvenem varstvu, so informacije, tehnologija in znanje (Hart, 2008). V literaturi lahko zasledimo, da je uporaba IT ena temeljnih kompetenc[3] medicinskih sester in daje pomembnost stroki, izboljšuje zdravstvo, dostop, učinkovitost ter kakovost (Bakken, 2006). Izraz IKT zajema poleg navedenega še prenos in uporabo vseh vrst informacij« (Čelebić in Rendulić, 2012, str. 1). IKT preoblikuje koncept zdravstvenega varstva ter znanstveno razumevanje človeškega telesa in bolezni. Je potencial za izboljšanje kakovosti in učinkovitosti oskrbe pacientov, odpira pa tudi pomembna etična in socialna vprašanja (Marckmann in Goodman, 2006).

Informatika je priljubljena tema v literaturi, medijih in izobraževanju. Strokovnjaki s področja zdravstvene nege pogosto ne razumejo omenjenega pojma (Dixon in Newlon, 2010). Identifikacija IKT kompetenc medicinskih sester je že vrsto let zanimiva tema. Raziskovalci v strokovnih organizacijah so te kompetence že opredelili (npr. Desjardins in sod, 2005; Hart, 2008; Westra in Delaney, 2008; Fetter, 2009a; Shultz, 2009). Slednje je treba vključiti v učni načrt zdravstvene nege in preko razvoja medicinskih sester zagotoviti delovno silo, ki bo usposobljena tudi na tem področju (Barton, 2005; Skiba in Rizzolo; 2009).

[3] Kompetence so merljivi standardi v strokovnem izobraževanju in praksi, ki se uporabljajo za določanje usposobljenosti posameznika za opravljanje določenih spretnosti (Shewchuk, O'Connor in Fine, 2005).

Iniciativa TIGER (angl. »The Technology Informatics Guiding Educational Reform«) je izdala priporočila (model) za medicinske sestre in študente zdravstvene nege, ki zajemajo tri področja, in sicer (TIGER, 2009):

- osnovne računalniške kompetence,
- informacijska pismenost[4] in
- upravljanje z informacijami (angl. »information management competencies«), ki zajema tri faze, in sicer: zbiranje podatkov, obdelavo podatkov ter predstavitev in sporočanje podatkov v obliki informacij in znanja. Najbolj relevantna, pomembna in temeljna sposobnost upravljanja informacij je tista, ki se nanaša na elektronske zdravstvene zapise (angl. »Electronic Health Records« - EHR). Tu je potrebno skrbno osredotočanje na zagotavljanje zaupnosti in zaščite pacientovih podatkov, zagotavljanje nadzora pri dostopu za uporabo zdravstvenega IS in zagotavljanje njegove varnosti.

Med IKT kompetence sodijo tudi kompetence s področja informacijske varnosti (AACN, 2011; Fetter, 2009b). Desjardins in sodelavci (2005) opozarjajo, da številni viri poudarjajo pomen omenjenih kompetenc. Podobno meni tudi O`Conor (2014). Mc Neil in sod. (2005) navajajo, da je zaradi slabega znanja s področja informatike posledično prisoten primanjkljaj tudi na področju informacijske varnosti. Omenjeni avtorji menijo, da k splošnim kompetencam medicinskih sester spadajo tiste, ki se nanašajo na oskrbo pacientov in zajemajo interpretiranje njihovih podatkov z različnimi aplikacijami, ki upoštevajo zasebnost/zaupnost in varnost podatkov v praksi. Varnost, povezana z informatiko na področju zdravstvene nege je ogrožena zaradi razmeroma visoke verjetnosti nepooblaščenega dostopa do podatkov (Damrongsak in Brown, 2008). Chang in sodelavci (2011) so na osnovni nivo kompetenc postavili informacijsko varnost. V eni izmed študij, izvedenih med podiplomskimi študenti zdravstvene nege, kjer so identificirali potrebne IKT kompetence medicinskih sester, so le redki prepoznali informacijsko varnost kot nujno potrebno znanje medicinskih sester pripravnic (Mc Neil in sod, 2005). V eni od navedenih študij je večina študentov navedla, da bi dodiplomski študijski program moral zajemati IKT znanja, pri tem pa je le peščica navedla poznavanje zasebnosti in varnosti zdravstvenih podatkov kot pomembno znanje medicinske sestre (Dixon in Newlon, 2010). V ZDA so opredelili okvir za integracijo vsebin IT (pridobivanje kompetenc) v učni načrt doktorata zdravstvene nege. Z integracijo vsebin želijo sedanje in bodoče medicinske sestre dobro pripraviti, saj ima sistem potencial za izboljšanje znanja in spretnosti v zdravstveni negi (Lilly in sod, 2015). IKT kompetence so pogoj za optimalno uporabo omenjenih tehnologij in za samo varnost pacientov (Desjardins in sod., 2005). Več strokovnih organizacij priporoča njihovo uporabo na vseh ravneh zdravstvenega varstva (AACN, 2011; IOM, 2010). Medicinske sestre morajo pri svojem delu znati uporabiti IKT za nemoteno delovanje v okoljih sodobne zdravstvene nege (Chang in sod., 2011). Te namreč zbirajo podatke ne samo od pacientov, temveč tudi iz drugih informacijskih virov. Iz navedenih informacijskih virov medicinska sestra uporabi informacije, ki jih potrebuje pri svojem delu (Niimi in Ota, 2014).

[4] Računalniška pismenost ali tehnološka pismenost je postala zelo pomembna v poklicu zdravstvene nege. Veščine informacijske pismenosti so potrebne za uspešno izvajanje pristopov, ki temeljijo na dokazih v klinični praksi, kot tudi za nadaljnji strokovni in osebni razvoj (Barton, 2005; Barnard in sod., 2005).

Albarrak (2011) v svoji študiji, ki je bila izvedena v King Saud University Hospitals (Savdska Arabija) na 900 medicinskih sestrah opozarja, da se omenjene zavedajo problematike informacijske varnosti, a kljub temu njihove navade predstavljajo resno grožnjo za varnost in zaupnost pacientovih podatkov. Študija poziva k dvigu ravni ozaveščenosti o informacijski varnosti med medicinskimi sestrami za zmanjšanje varnostnih groženj, ki jih predstavljajo nedostojna vedenja uporabnikov. To se npr. kaže v visokem deležu medicinskih sester, ki ne spremenijo svojega gesla tudi potem, ko je postalo znano (Albarrak, 2011). V zadnjih letih je upravljanje z zdravstvenimi informacijami z uporabo IKT občutno napredovalo. Zdravstvene ustanove so z uvajanjem IKT pridobile veliko prednost, ki se kaže v optimizaciji dela, zmanjševanju stroškov, izmenjavi informacij, izboljšanju varnosti (Niimi in Ota, 2014).

IKT pripomore k drugačni uporabi zdravstvene storitve s tem, da poveča dostopnost do informacij in zagotovi druge oblike podpore na daljavo. V 21. stoletju je kakovostne zdravstvene storitve možno zagotoviti samo z ustrezno uporabo IKT v praksi (Albarrak, 2012). Uporaba IKT prinaša tudi možne prednosti in slabosti zdravstvenih storitev (While in Dewsbury, 2011). Pojavljajo se vprašanja o tem, kako ravnati z osebnimi podatki (v nadaljevanju OP) pacientov in kako zagotoviti njihovo varnost in zasebnost (Niimi in Ota, 2014). Ni treba poudarjati, da zdravstvene ustanove razpolagajo z ogromnimi količinami zaupnih pacientovih podatkov. Ti ne vključujejo le imen in naslovov, temveč tudi zasebne podatke, zato je treba z njimi ravnati previdno (Niimi in Ota, 2014). Medicinske sestre pri odpustitvi pacienta iz bolnišnice sporočajo podatke bivanja pacienta različnim zdravstvenim delavcem. Takšno ravnanje omogoči velikemu številu nepooblaščenih oseb dostop do informacij in ustvarja veliko tveganje za kršitve zaupnosti (Kummeth in sod., 2007). Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki so povezane z obdelavo OP, so dolžni varovati tajnost OP, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti OP jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del, nalog ali storitev pogodbene obdelave (ZVOP, 2007, str. 12711). Zagotovilo, da so podatki vedno v pravih rokah, je ključnega pomena za ohranjanje zaupanja med medicinsko sestro in pacientom, kar narekuje tudi III. načelo Kodeksa etike medicinskih sester (Ovijač in sod., 2014). Dolžnost in profesionalna obveznost medicinskih sester je varovati podatke o pacientih. Te si morajo prizadevati za ohranjanje zaupanja z besedami in dejanji (Griffith, 2007). Ne glede na opisano pa je za učinkovito izvajanje zdravstvene nege in izogibanje tragediji ter slabi oskrbi pomembna prav izmenjava podatkov znotraj tima (Griffith, 2007).

IKT olajša izvajanje zdravstvene nege, povečuje čas, preživet v neposredni oskrbi pacientov, izboljšuje odločanje, zmanjšuje podvajanje dela, napak in časa, ki se ga porabi za izpolnjevanje dokumentacije (Chang in sod., 2011, Dowding, 2013).

V nadaljevanje bomo predstavili le peščico etičnih vidikov, s katerimi se srečujejo medicinske sestre na delovnem mestu v povezavi z elektronskim okoljem.

- Odjava računalnika: delovne postaje z računalnikom – omejen dostop. Odjava ali zaklepanje delovne postaje ali računalnika ob začasni odsotnosti ali če ga trenutno ne potrebujemo. Načina zagotavljata zaupnost podatkov in tako varujeta tudi zaposlene, saj onemogočata nepooblaščenim osebam vnos podatkov ali naročil ter iskanje informacij pod drugim uporabniškim imenom (Kummet in sod., 2007).

- Dostop do informacij le na podlagi potrebe po seznanitvi: samo zato, ker imajo medicinske sestre omogočen dostop do podatkov, še ne pomeni, da lahko pogledajo v zdravstveno kartoteko. Pred dostopom do elektronskega zapisa je potrebno premisliti, ali imamo utemeljene razloge za to (Kummet in sod., 2007). Obstaja namreč sistem sledljivosti, s katero se ugotavlja, kdo je zlorabil določene OP. Kot primer izpostavimo, da v javnost »pricurljajo« podatki o zdravstvenem stanju medijsko izpostavljene osebnosti. Sistem zabeleži, kdo/kdaj je do podatkov dostopal ter ali jih je dopolnil in spremenil (Informacijski pooblaščenec v sodelovanju s skupino za bolnišnične informacijske sisteme pri združenju zdravstvenih zavodov Slovenije, 2008, str. 6).
- Uporaba drugih naprav: kako je treba zagotoviti varnost podatkov, če so na različnih napravah? Kako je treba ravnati s podatki, ki jih ne potrebujemo več in čemu uporaba naprav za razrez dokumentov? Kakšna je trenutna praksa in kakšni so vzpostavljeni zaščitni ukrepi za zagotovitev zaupnosti pri prejemanju informacij pacientov preko faksa (Kummet in sod., 2007)?

1.2 Opredelitev informacijske varnosti in zasebnosti

Kovačič (2006) je zapisal, da univerzalne definicije zasebnosti in pravice do zasebnosti ni, ker je subjektivna in ima vsakdo zanjo drugačna pričakovanja (Kovačič, 2006, str. 12). Brezovšek in Črnec (2007) navajata, da je informacijska zasebnost (pravica do zasebnosti) sinonim za varstvo osebnih podatkov[5] in ena od sestavin zasebnosti. Prav tako sta zapisala stari pregovor, ki pravi: »Kdor ima informacijo, ima tudi moč«. Danes to velja bolj kot kadarkoli v zgodovini, saj IKT omogoča posameznikom, skupinam in organizacijam, da obdeluje in shranjuje ogromne količine OP (Brezovšek in Črnec, 2007, str. 195,196). Varnost in kakovost življenja sta v današnji informacijski družbi odvisna od IKT. Zaradi njene uporabe se postavlja vrsta varnostnih vprašanj, strah pred nevarnostmi pa zavira razvoj celotne družbe (Bratuša, 2010). Zloraba zasebnosti na internetu je podobna tisti v fizičnem svetu s to razliko, da se kaže drugače in da zaradi pogoste uporabe IKT prihaja do nje pogosteje. Informacijska in komunikacijska zasebnost se varujeta s tajnostjo. Zato velja kriptografija[6] za eno poglavitnih tehnologij zaščite zasebnosti na internetu (Kovačič, 2006, str. 8, 12, 44). Na žalost se večkrat zgodi, da zdravstveni delavci poleg svojih osebnih zadev delijo na družabnih omrežjih tudi razne informacije, povezane z delom (NRC, 2011). Takšna dejanja imajo lahko posledice, ki se jih zaposleni sploh ne zavedajo (npr. morebitne tožbe).

Informacijska varnost je opredeljena kot (Čelebić in Rendulić, 2012, str. 28):

- ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij;
- varnostni ukrepi informacij, ki so pravila o varstvu osebnih podatkov na fizični, tehnični in organizacijski ravni.

[5] Varstvo osebnih podatkov je kategorija, ki se v širšem kontekstu umešča v širši okvir imenovan zaščita podatkov. Zaščita podatkov obsega varstvo osebnih podatkov oz. varstvo posameznikove informacijske zasebnosti in zavarovanje podatkov (Brezovšek in Črnec, 2007; str. 196).

[6] Kriptologija je veda o tajnosti, šifriranju (enkripcija), zakrivanju sporočil in razkrivanju šifriranih podatkov. Osnovno sporočilo je čistopis, zašifrirano pa šifropis ali tajnopis. Sporočilo se po postopku (algoritmu) spremeni v kriptirano sporočilo. Pri tem se za določene vrednosti uporabijo parametri v algoritmu, ki se jim reče ključ (Verdonik in Bratuša, 2005, str. 193).

Informacija lahko obstaja v različnih oblikah. Ne glede na obliko informacije mora biti ta vedno ustrezno zavarovana (Bernard, 2007). Brezovšek in Črnec (2007, str. 115,116) navajata, da sam tajni podatek ne pomeni veliko, če ni vzpostavljen celotni sistem ravnanja s tajnimi podatki. Poleg tehničnih, fizičnih in organizacijskih ukrepov, ki so vzpostavljeni za izvajanje varovanja tajnih podatkov, je največjo pozornost treba nameniti pravilom za dostop do njih. Zavarovanje OP je urejeno v 24. členu ZVOP (2007, str. 12711) in določa, da zavarovanje OP obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo OP, preprečuje naključno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava na način, da se:

- varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;
- varuje aplikativna programska oprema, s katero se obdelujejo OP;
- preprečuje nepooblaščen dostop do OP pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja OP;
- omogoča poznejše ugotavljanje, kdaj so bili posamezni OP vneseni v zbirko, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je možno zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave OP.

Informacijska varnost ni le varnost informacij samih. Njena zloraba in neustrezno zagotavljanje (zlorabe tehnologije, nepooblaščen dostop v omrežje bolnišnice) lahko privede do smrti. Leta 2006 je v Beatson Oncology Centru v Glasgowu zaradi napačnih preračunavanj odmerkov sevanja življenje izgubila 16 let stara oseba (Bratuša, 2010). Znan je tudi primer nepooblaščenega dostopa v zaščiteno zbirko Ginekološke klinike Ljubljana iz leta 2000. Neznani storilec je vdrl v spletni strežnik klinike in prenesel podatke s spletnega strežnika. Ti so vsebovali uradno spletno stran klinike, telefonski in elektronski imenik zaposlenih, podatkovne zbirke s podatki o zdravnikih in pacientkah, knjige v elektronski obliki in različno testno programsko opremo (Verdonik in Bratuša, 2005, str. 222-224). Občutljivi OP v pravih rokah so ključnega pomena, v napačnih rokah pa lahko povzročijo raznovrstno škodo, uničijo ugled organizacij in povzročijo stroške (NRC, 2011). Zavarovanje občutljivih OP je posebej urejeno v 14. členu ZVOP in določa, da morajo biti občutljivi OP pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih (ZVOP, 2007).

Grožnje varnosti razvrščamo v naslednje skupine (Cunningham in sod., 2007):

- človekova zlonamerna dejavnost (npr. sabotaža, vandalizem, vlom, kraja, podtaknjen požar/ogenj/požig, nasilje na delovnem mestu, spori med delovno silo, kemične in biološke nevarnosti, terorizem, vojna, civilni nemiri, itn.);
- grožnje, ki pretijo infrastrukturi (npr. netehnološka oprema, odpoved sistema, izpad električne energije, ogrevanje/hlajenje, poškodbe poslovne stavbe, odpoved podporne tehnologije, izliv vode, potres itn.) in
- grožnje, specifične za informacijsko tehnologijo (kibernetske grožnje, okvare opreme ali sistemske okvare, programski vsiljivci, vdor, izguba podatkov in zapisov itn.).

Pogosto se grožnje delijo tudi v naslednje tri skupine (Brezavšček in Moškon, 2010):

- izredni dogodki,
- naključni dogodki in
- človekova (zlo)namerna dejavnost.

Varnostnih zahtev ni mogoče obravnavati samo s tehnologijo. Grožnje informacijske varnosti ni mogoče preprečiti, se jim izogniti, jih zaznati ali odpraviti izključno s poudarkom na tehnoloških rešitvah. Pomemben vidik zaščite je odvisen od odnosa, zavesti, vedenja in sposobnosti vpletenih oseb (Furnell in sod., 2006; HAISA, 2007; Trček in sod., 2007; Herath in Rao, 2009). Pincus (2005) in drugi avtorji že več let vztrajajo pri tem, da je človeški faktor enako ali celo bolj pomemben pri doseganju in sprejemanju ravni informacijske varnosti v organizaciji. Ključen dejavnik tveganja pri varovanju tajnih podatkov ostaja nedvomno človek (Brezovšek in Črnec, 2007, str. 116).

V nadaljevanju so našteti nekateri človeški dejavniki, ki lahko vplivajo na varnost IS organizacije (Pattinson in Anderson, 2007). Nekateri se nanašajo na okolico, drugi pa so sociološki in povezani z vzgojo, kulturo ter izkušnjami:

- organizacijska politika in varnostna kultura;
- posameznikova nagnjenost k tveganju;
- teorija homeostaze tveganja;
- vpliv opazovalca/drugi navzoči;
- poznavanje/seznanjenost s komunikacijo;
- posameznikova zaznava tveganj;
- starost, spol, položaj v organizaciji;
- stroški skladnosti;
- kakovost izobraževanja in usposabljanja;
- individualni kognitivni stil;
- izkušnje in
- poročanje o tveganjih (kako dobro se poroča o tveganjih).

Bernik in Prislan (2013) sta v svoji raziskavi, izvedeni leta 2010, preverila razumevanje informacijske varnosti in z njo povezanega sistema upravljanja s tveganji. Primerjala sta 18 organizacij iz različnih segmentov gospodarstva, zasebnega in javnega sektorja, ki zaposlujejo do 50 zaposlenih. Rezultati so pokazali, da grožnje informacijske varnosti pri večini organizacij niso ustrezno razumljene, proces upravljanja s tveganji pa je odvisen od vsake od njih. Kot problem sta izpostavila število sistemov za upravljanje s tveganji, ki jih je veliko. Več kot polovica tj. 60 % meni, da varstvo podatkov predstavlja kritično točko pri uspešnem poslovanju. Presenetljivo je mnenje nekaterih organizacij, da je pri tem pomembna samo strojna oprema. Varovanje podatkov s sodobnimi tehnikami in z višjimi standardi ima 28 % organizacij (npr. kontinuirana politika, digitalna potrdila) (Bernik in Prislan 2013). Številne organizacije v tujini izvajajo letne raziskave s področja informacijske varnosti. Tako beležijo kršitve in njihov vpliv, ne poskušajo pa ugotoviti, kaj na to pravijo oz. kakšna so mnenja uporabnikov računalnikov ali kaj vedo/počnejo za varnost informacij (Deloitte, 2011; Ernst in Young, 2011;). Kar nekaj študij, ki raziskujejo vedenja uporabnikov računalnikov, se osredotoča le na eno komponento zavedanja informacijske varnosti. Stanton in sodelavci (2005) so raziskovali vedenja, povezana z varnostjo gesel. Mylonas

in sodelavci (2013) so preučili omenjeno problematiko na mobilnih IKT. Da bi ovrednotili ranljivost informacijske varnosti s strani človeškega vedenja, so Parsons in sodelavci (2014) razvili vprašalnik za prepoznavanje človeškega vidika informacijske varnosti (angl. »Human Aspects of Information Security Questionnaire - HAIS-Q«). Rezultati njihove raziskave, ki je zajela 500 avstralskih zaposlenih, je pokazala, da ima poznavanje politike in njenih postopkov močan vpliv na informacijsko varnost. Ugotovili so, da sta usposabljanje in izobraževanje (znanje) učinkovitejši, če je prisotno tudi razumevanje pomena odnosa do informacijske varnosti (Parsons in. sod, 2014).

Šolić in sodelavci (2014) so sestavili vprašalnik UISAQ (angl. »User's Information Security Awareness Questionnaire«), čigar namen je bil razviti univerzalni instrument za merjenje ravni ozaveščenosti o informacijski varnosti. Preliminarni rezultati uporabe omenjenega vprašalnika pri študentih treh različnih fakultet so pokazali, da je lahko UISAQ dober in zanesljiv ukrep ozaveščenosti o informacijski varnosti (Šolić in sod., 2014). Omenjeni avtorji so v svojem prispevku predlagali model za oceno varnostnih vprašanj in zgradili ontologijo[7] uporabnikovega potencialnega tveganega vedenja pri uporabi elektronske pošte. Uporaba ontologije za formalizacijo tveganega vedenja se je izkazala kot obetavno orodje, ki zajema celovit pristop k informacijski varnostni politiki (Šolić in sod., 2010).

Vzdrževanje ustrezne ravni informacijske varnosti je neskončen proces, saj se število groženj neprestano povečuje. Vzpostavitev informacijske varnosti ni zgolj uvajanje novih varnostnih tehnologij, temveč vključuje tudi usmeritve, postopke in ukrepe, ki skrbijo, da ostanejo podatki zaupni in so na voljo tistim, ki jih potrebujejo (Glaser in Aske, 2010). Zaradi potrebe po izboljšani informacijski varnosti so mnoge organizacije vzpostavile programe ozaveščanja o varnosti informacij, da bi zagotovile obveščenost in ozaveščenost zaposlenih o varnostnih tveganjih (Kruger in Kearney, 2006). Da bi program ozaveščanja o varnosti imel dodano vrednost za organizacijo in hkrati prispeval na področju informacijske varnosti, je treba imeti niz metod za preučevanje in merjenje njegovega učinka (Kruger in Kearney, 2006). Medtem ko se informacijska varnost na splošno osredotoča na varovanje zaupnosti, celovitosti in razpoložljivosti informacij, se zavedanje informacijske varnosti nanaša predvsem na ozaveščanje pri uporabi programov, za ustvarjanje in ohranjanje varnosti ter pozitivno mnenje, ki je kritični element učinkovitega informacijskega varnostnega okolja (Kruger in Kearney, 2006).

1.3 Varovanje pred osebjem

Pri razvoju različnih informacijskih varnostnih rešitev je potrebno upoštevati vedenjsko vlogo uporabnikov IKT, saj lahko le-ti bistveno ogrozijo varnost IS na več načinov (Verdonik in Bratuša, 2005, str. 192; Šolić in sod., 2013). Zaposleni so lahko namerno ali iz malomarnosti ter pogosto zaradi pomanjkanja znanja največja grožnja varnosti informacij (Niekerk in Solms, 2010). Spet drugi lahko izpostavijo k razkritju občutljiva sredstva, celovitost informacij ali blokirajo razpoložljivost kritičnih sistemov (Landoll, 2006, str. 154). Nekateri uporabniki so neizučeni ali nevešči uporabe računalnika in tako uničijo ali poškodujejo podatke. Drugi to storijo namerno, v svojo korist,

[7] Je filozofska disciplina, ki obravnava osnovo, vzroke in najsplošnejše lastnosti stvarnosti (SSKJ, 2000). Ontologija se uporablja za formalno določanje znanja o nekaterih področjih zanimanja, ki opredeljuje pojme in odnose med njimi (Šolić in. sod, 2010).

kriminalne skupine pa jih spreminjajo in medsebojno prodajajo. Vse naštete grožnje in nevarnosti so odvisne od naslednjih naštetih dejavnikov (Verdonik in Bratuša, 2005, str. 192):

- Dostop[8] – škoda je odvisna od omejenosti vstopa v IS in od avtorizacije uporabnika za dostop. Upoštevati je treba uporabnikov dostop do glavnega računalnika, terminala ali do programske opreme;
- Znanje – večje kot je znanje uporabnika, večja je možnost ogrožanja. Na drugi strani pa neznanje in ignoranca prav tako pomenita nevarnost;
- Motivacija – največja nevarnost na tem področju so zaposleni, ki imajo neposreden dostop do sistema. Za zaščito je pomembno njihovo preverjanje (preteklost), nadzorovanje, usposabljanje in odgovornost. Nevarnost predstavljajo vzdrževalci in prodajalci IKT.

1.4 Vedenja uporabnikov

Veliko strokovnjakov s področja informacijske varnosti je prepričanih, da spodbujanje dobrih in omejevanje slabih uporabnikov zagotavlja eno najpomembnejših metod za vzpostavitev organizacijskega efektivnega IS (Stanton in. sod, 2005). V preglednici 1 so predstavljena vedenja uporabnikov računalnikov/zaposlenih, ki največkrat niso škodoželjna organizaciji ali njenim virom. Povezana so z naivnostjo ali nevednostjo. Vrsto takih vedenj so Stanton in sodelavci (2005) poimenovali kot naivne napake. Razvili so taksonomijo[9] šestih vedenjskih kategorij. Ta je prikazana v preglednici 2 Herath in Rao (2009) so v svoji študiji preučili potencialni vpliv spremenljivk, kot so npr. normativna prepričanja ali namere, ki zadevajo varnostno politiko. Nobena od raziskav pa ni poskušala ugotoviti, kakšna je splošna ozaveščenost zaposlenih o informacijski varnosti. Parsons in sodelavci (2014) so prepričani, da povezava med znanjem, odnosom in vedenjem vpliva na posameznika, posredovanje in organizacijske dejavnike/faktorje. Na primer, psihološki dejavniki (usposabljanja, udeležbe na seminarjih) in organizacijska informacijska varnostna kultura, ki jo raziskujeta Veiga in Eloff (2010), imajo potencialni vpliv na znanje, odnos in vedenje zaposlenih. Informacijsko varnostno kulturo raziskujeta tudi Niekerk in Solms (2010), ki poudarjata, da je ta ključnega pomena za upravljanje človeških dejavnikov, ki sodelujejo na področju informacijske varnosti.

Vsaka zdravstvena organizacija mora zagotoviti, da bodo vse informacije zasebne in varne. Sprejeti mora različne pristope za razvoj zasebnosti in varnostne politike ter tako ustvariti zaupanja vredno okolje (Dimitropoulos in Rizk, 2009). Osredotočiti se mora na vedenje zaposlenih, saj je prav od njih odvisen ugled organizacije (Veiga in Eloff, 2010). Pahnila in sodelavci (2007) so v svoji raziskavi potrdili, da ima kakovost informacij pomemben vpliv na varnostno politiko IS. Omenjeni avtorji navajajo, da imajo odnos, normativna prepričanja in navade prav tako pomemben vpliv na namero izpolnjevanja varnostne politike.

[8] Pri nadzoru dostopa in omejitvi uporabnika glede na potrebe in pooblastila se v IKT uporabljajo tri orodja pod kratico AAA (ang. »authentication, authorization, accounting«). To so: preverjanje pristnosti (določi identiteto), pooblaščenje (določi do česa lahko uporabnik dostopa) in vodenje računov (orodje, ki preverja zgoraj naštete postopke) (Egan in Mather, 2005, str. 33).
[9] Nauk o razvrščanju in poimenovanju (SSKJ, 2000).

Preglednica 1: Vedenja uporabnikov računalnika (angl. »Behavior of computer users«) (Stanton in sod., 2005)

Območje (področje)	Dobro vedenje (primerno)	Nevtralno vedenje (nezgode/nesreče)	Slabo vedenje (neprimerno)
Upravljanje z gesli	Odjava iz IS v primeru zapuščanja delovne postaje	Delitev uporabniških imen in gesel	Vdor v račune drugih uporabnikov
Uporaba elektronske pošte	Zavrnitev priponk neznanih pošiljateljev	Odpiranje nepričakovanih in neznanih el. pošt	Ustvarjanje in pošiljanje spama[10]
Uporaba interneta	Uporaba pooblaščene programske opreme	Dostop do sumljivih spletnih strani	Prenašanje video vsebin na služben računalnik
Uporaba družabnih spletnih strani	Izogibanje v službenem času	Nezavedanje posledic objave podatkov	Objavljanje občutljivih informacij o delovnem mestu
Poročanje o incidentih	Pozornost in kritičnost pri prepoznavanju približevanja nepooblaščenih oseb	Neporočanje o varnostnih incidentih	Dopuščanje nepooblaščenim osebam dostop do pooblaščenih prostorov/območij
Mobilno računalništvo	Pošiljanje elektronskih sporočil samo preko varnih omrežij	Službeni prenosnik/dlančnik pušča brez nadzora	Konfiguriranje brezžičnega omrežja, ki omogoča nepooblaščen dostop
Rokovanje z informacijami	Uničenje občutljivih dokumentov, ki niso več uporabni	Puščanje nosilcev ali dokumentov z občutljivimi podatki na mizi brez nadzora	Pisanje in širjenje zlonamerne kode

Organizacije imajo različne načine shranjevanja in zaščite kritičnih informacij (varnostna kopija, dvojne lokacije, arhiviranje, posebni strežniki). Najpogostejše grožnje, kot so zlonamerne kode (virusi, napake strojnih oprem itn.), lahko s pomočjo protivirusnih programov in požarnih zidov ali s primernim kopiranjem podatkov enostavno in relativno poceni omilimo. Večja nevarnost še vedno ostaja človeški faktor. Uporabniki so najpogosteje glavna grožnja IS, predvsem zaradi pomanjkanja znanja in zavesti o tem, kako pomembna je zaupnost podatkov (Bernik in Prislan, 2013). Neprevidni zaposleni večkrat niso v skladu z varnostno politiko in njenimi postopki (Pahnila in sod., 2007). Njihova vedenja vključujejo namerna in nenamerna razkrivanja uporabniških gesel, nepozornost pri uporabi elektronske pošte in uporabe nosilca podatkov v službi ali doma (Parsons in sod., 2014).

Krivec za kršitev informacijske varnosti je vedenje zaposlenih, ki se kaže predvsem pri neizbiri močnega gesla in odpiranju sumljivih priponk (Ng in sod., 2009). Nepoznavanje tega področja je razvidno iz mnenja posamezne organizacije, da so najhujše grožnje virusi, sistemske napake, vlomi, okvare in začasno nedostopni sistem (Bernik in Prislan, 2013). Zaradi tega je treba spremeniti dojemanje informacijske varnosti iz tehničnega vidika do točke uporabnikovega stališča (Bernik in Prislan, 2013).

[10] Neželena elektronska pošta (angl. »spam«). Gre za nezahtevano komercialno elektronsko pošto. Uporablja se tudi okrajšava UCE (angl. »Unsolicated Commerccial Email«). Je dokument poslan po elektronski pošti in vsebuje podatke o prodaji, najemu, darovanju blaga, nepremičnin in storitev, naslovljeno na prejemnika, ki nima neposrednega poslovnega ali osebnega odnosa s prejemnikom in ni bil poslan na njegovo zahtevo ali po njegovi privolitvi (Verdonik in Bratuša, 2005, str. 129).

Preglednica 2: Faktorja taksonomije varnostnih vedenj (Stanton in sod., 2005)

Strokovne namere	Primer	Opis
Visoke zlonamerne	Namerno uničenje	Vedenje vključuje tehnično strokovno znanje, skupaj z močno namero škodovanja organizacijski IT in njenim virom. Primer: zaposleni vdre v zaščitene datoteke delodajalca, da bi ukradel poslovne skrivnosti.
Nizke zlonamerne	Škodljiva zloraba	Vedenje vključuje minimalno tehnično znanje in zajema namero škodovanja skozi nadlegovanje in kršenje pravil. Primer: uporaba službene e-pošte za pošiljanje SPAM sporočil.
Visoke nevtralne	Nevarno »igračkanje«	Vedenje zajema tehnično znanje, brez jasne namere škodovanja organizacijski IT in njenim virom. Primer: zaposleni delavec nastavi brezžični prehod, ki omogoča brezžični dostop do omrežja organizacije, v kateri je zaposlen.
Nizke nevtralne	Naivne napake	Vedenje zajema minimalno tehnično znanje in nobenega jasnega namena škodovanja organizacijski IT in njenim virom. Primer: izbira slabega gesla.
Visoke koristne	Zavedanje varnosti	Vedenje zajema tehnično strokovno znanje, skupaj z močno namero delati dobro, z ohranjanjem in zaščito organizacijske IT in njenih virov. Primer: zaposleni prepozna škodljive programe s skrbnim opazovanjem lastnega računalnika.
Nizke koristne	Osnovna higiena	Vedenje ne zajema tehničnega znanja, temveč vključuje jasno namero za ohranitev in zaščito organizacijske IT in njenih virov. Primer: usposobljeni in seznanjeni zaposleni se upira poskusu socialnega inženiringa.

1.5 Fizična zaščita

Osnova varovanja pred računalniškim kriminalom je fizična zaščita. Z ukrepi se varuje pred naravnimi in drugimi nesrečami, namernim poškodovanjem opreme in tatvino. Preprečujejo se katastrofe ali vsaj zmanjša njihov učinek (Verdonik in Bratuša, 2005). Za pooblaščen vstop mora uporabnik pokazati avtentičnost (prepoznavanje identitete ali pristnosti), kar lahko stori (Egan in Mather, 2005; Verdonik in Bratuša, 2005):

- s poznavanjem enega od podatkov (geslo),
- s kodiranim predmetom (ključ, magnetna kartica),
- s prstnim odtisom ali preko očesne mrežnice in
- z ugotavljanjem položaja s sateliti.

Preglede je treba izvajati redno, nujno je tudi sistematično preverjati ali zaposleni upoštevajo varnostne ukrepe za fizično varovanje ter na močno izpostavljenih točkah preizkušati možnost vdora. Pozornost mora biti usmerjena na vhode v prostor z opremo. Prezračevalni sistemi morajo biti zavarovani, računalniki pa ne smejo biti postavljeni zraven oken (Verdonik in Bratuša, 2005). Pozornost mora biti usmerjena tudi na odpadke (papir) v koših za smeti, saj se tam pogosto znajdejo vstopna gesla in drugi pomembni podatki. Na vhodih je treba poostriti varovanje z varnostniki in napravami z videonadzorom. Koristna je namestitev preverjanja identitete ob vstopu v prostor

(magnetne kartice, preverjanje prstnih odtisov, glasu, ročnih podpisov, očesne mrežnice) (Verdonik in Bratuša, 2005).

1.6 Varnostno kopiranje osebnih podatkov

Način, na katerega ljudje vidijo tveganje povezano z informacijsko varnostjo določa, kakšne odločitve in ukrepe bodo sprejeli/ne-sprejeli v povezavi s katerim koli varnostnim ukrepom, ki ga ima organizacija vzpostavljenega. Do danes ni veliko znanega o zaznavanju in dojemanju uporabnikov v zvezi s tveganjem IS (Pattinson in Anderson, 2007). Poglejmo dober praktičen primer dojemanja tveganja, ki se nanaša na varnostno kopiranje osebnih podatkov. Na delovnem mestu se več dni posvečate pisanju zelo pomembnega poslovnega poročila/raziskovalnega dela za vašega nadrejenega/vodstvo organizacije. Kako pogosto boste naredili kopijo (ang. »backup[11]«) svojega dela? Kakšno je tveganje, da boste izgubili vse svoje delo zaradi nedelovanja računalnika? Veliko ljudi podcenjuje kompleksnost računalnika in se zato ne zaveda tveganja. Na drugi strani, pa so ozaveščeni tisti, ki se zavedajo nepredvidljivosti računalnika. Ti svoje podatke kopirajo redno in v različne nosilce (Pattinson in Anderson, 2007). Bergen (2005) v svojem članku, v katerem piše o zaščiti integritete elektronskih študentskih zdravstvenih zapisov navaja, da lahko varnostno kopiranje podatkov primerjamo z dnevno zobno higieno ter da mnogi zdravstveni delavci zanemarjajo to nalogo.

1.7 Gesla

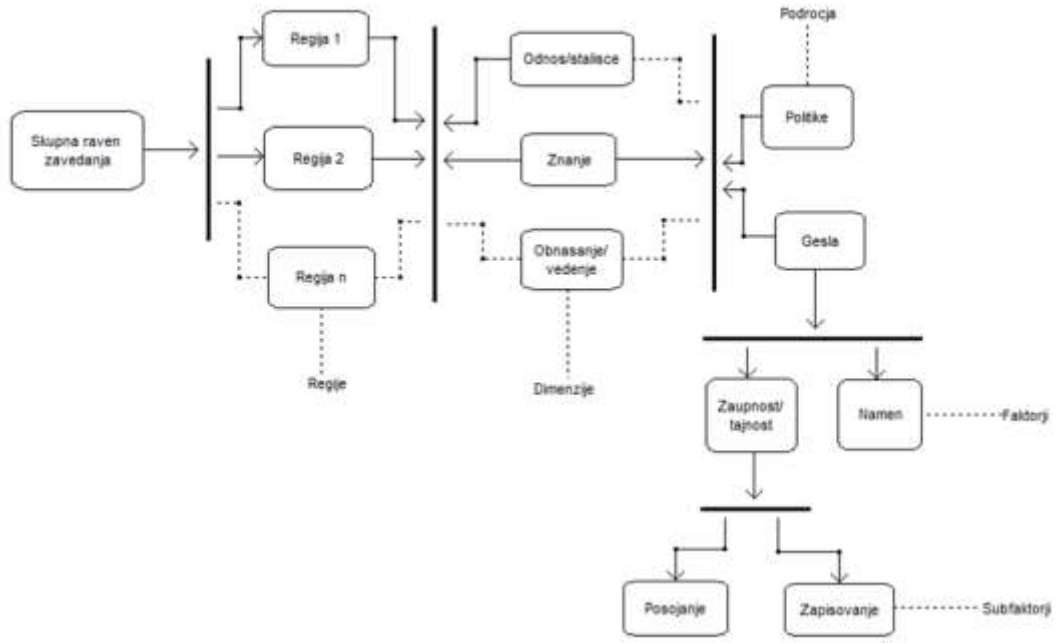
Avtentifikacija je identifikacija uporabnika, ki omogoča dostop do določenih podatkov (npr. za dostop do el. pošte je potrebno vnesti uporabniško ime in geslo). V kolikor je preverjanje uspešno, se pristop odobri. Zaradi varnostnih razlogov morajo gesla ostati zaupna. Geslo ni nič drugega kot ključ za dostop do doma ali avta (Čelebić in Rendulić, 2012). Varnost je kršena, ko nepooblaščeni uporabnik dobi dostop do sredstev, ali ko preseže dodeljeno raven dostopa do zavarovanega sistema (Egan in Mather, 2005). Poglejmo si primer skupne ravni zavedanja zaposlenih. Metodologija, ki sta jo Kruger in Kearney (2006) razvila za razvoj merilnega orodja, temelji na tehnikah, izposojenih na področju socialne psihologije.

Prva klasifikacija je razdeljena na tri dimenzije:

- spoznanje/znanje (kaj znaš),
- odnos (kaj misliš) in
- vedenje/obnašanje (kaj narediš).

Druga klasifikacija je osredotočena na specifična področja (glej sliko 1). Če pogledamo področje »gesel«, je to razdeljeno v dve kategoriji, in sicer: namen in zaupnost gesla. Zaupnost gesla pa je razčlenjena na zapis gesla ali posojanje gesla drugim. Gesla so postala nujen del vsakdana za nadzor dostopa do sistemov in aplikacij, ki upravljajo z digitalnimi informacijami.

[11] Postopek, s katerimi se iz prvotnih podatkov (datoteke, programi) naredi kopija. S tem izvornik zaščitimo pred izgubo podatkov ali izbrisom. Elektronske podatke lahko shranimo na trdi disk, DVD, CD, USB ključek, itn. (Čelebić in Rendulić, 2012, str. 29).



Slika 1: Strukture problemov (Kruger in Kearney, 2006)

Rast IKT zahteva uporabo gesel kot osnovno orodje za zaščito digitalnih informacij (Weber in sod., 2008). Egan in Mather navajata, da so uporabniška imena in gesla najosnovnejša oblika preverjanja pristnosti in so elektronski ključ za vstop v sisteme za varovanje informacij (Egan in Mather, 2005, str. 33). Vsak računalnik mora biti vedno zaščiten z geslom (NRC, 2011).

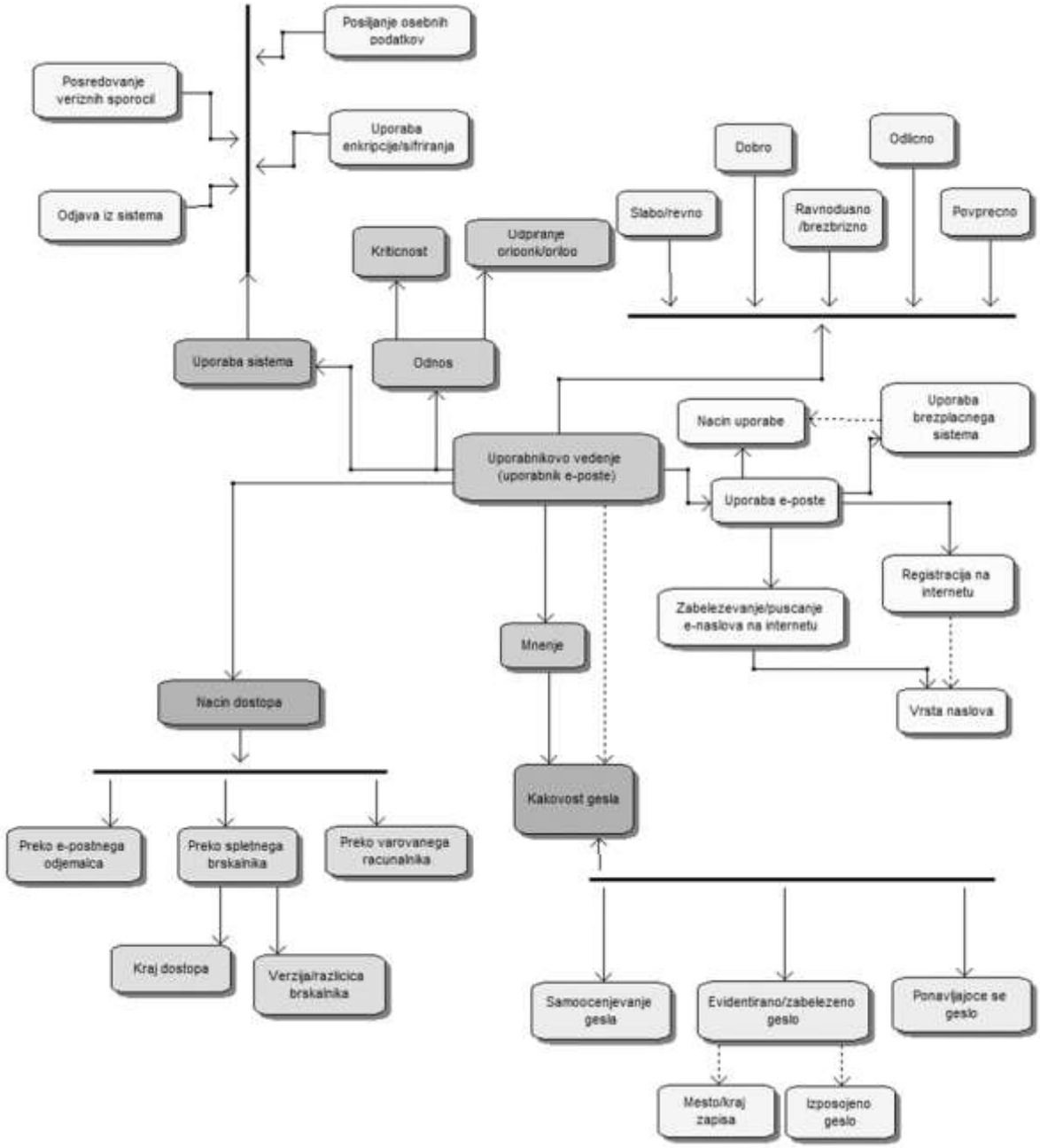
1.8 Elektronska pošta

E-poštni sistem je dinamičen del sistema IKT in se ves čas razvija. Brezplačne spletne e-poštne storitve (npr. Gmail, Yahoo in Hotmail) so po vsem svetu znane in uporabljene za osebno in strokovno komunikacijo (Šolić in sod., 2010). Bratuša (2007, str. 117) je opredelil metode za napad na sistem elektronske pošte, ki so: priponke s škodljivo vsebino, e-pošta kot posrednik za izkoriščanje varnostnih vrzeli, e-pošta, napisana v obliki HTML in vanjo vgrajena škodljiva koda, socialni inženiring in t. i. ribarjenje ter preostale metode izogibanja protivirusnim programom in filtrom. E-poštni komunikacijski kanal je v zadnjih letih močno prekinjen zaradi zlonamernih napadov (Šolić in. sod, 2013). Neželena elektronska pošta zajema 80 % celotnega prometa elektronske pošte na internetu (Bratuša, 2007, str. 16). Ob nastanku računalnikov so virusi bili le igrače najstnikov, danes so zaslužek kriminalcem (Bratuša, 2010). Zatiskanje oči organizacij pred krajo podatkov in zaupnih informacij je nedopustna. Zaposleni pogosto uporabljajo elektronsko pošto za pošiljanje zaupnih dokumentov in informacij. E-pošto uporabljajo tako uslužbenci kot tudi osebe, ki se pomena posameznih informacij in načina delovanja e-pošte ne zavedajo (Verdonik in Bratuša, 2005).

Statistični podatki kažejo, da se v strokovnih organizacijah večina kršitev varnosti uporabnikom zgodi ne zlonamerno. Zaradi tega je treba posebno pozornost nameniti uporabi e-pošte in zaposlene usposobiti za uporabo osnovnih znanj s področja varnosti IKT (Šolić in sod., 2013). Informacijski pooblaščenec priporoča opredelitev uporabe interneta in e-pošte v internem aktu (primer: Pravilnik o zavarovanju OP). Delodajalčeva dolžnost je nadzor nad delovnimi sredstvi. Na drugi strani pa je pravica do zasebnosti, ki jo v določeni meri uživa zaposleni, tudi na delovnem mestu temeljna. Tako prihaja do kolizije legitimnih interesov (Informacijski pooblaščenec v sodelovanju s skupino za bolnišnične informacijske sisteme pri združenju zdravstvenih zavodov Slovenije, 2008, str. 10). Ko se občutljivi podatki prenašajo po omrežju, so lahko dovzetni za napade. Tehnični zaščitni ukrepi, kot so šifriranje omrežja, virtualna zasebna omrežja in šifriranja e-poštnih sporočil lahko pomagajo varovati zaupnost in neoporečnost podatkov (Landooll, 2006).

V primeru obdelave OP, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativna programska oprema zagotavljati, da je obdelava OP v zbirkah OP v mejah pooblastil uporabnika OP. Pri prenosu občutljivih OP preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom (ZVOP, 2007, str. 12711).

Osnovni elementi ontologije (glej sliko 2) pri uporabnikovem tveganem vedenju in možnih varnostnih vprašanjih v zvezi z uporabo e-pošte, so uporaba nezaščitenega računalnika, manj varnega spletnega brskalnika ali brskalnika starejše verzije, ne-šifriranje občutljive e-pošte, odpiranje prilog neznanih pošiljateljev in nekritičnost. Sem sodi tudi odgovarjanje na »lažno« e-pošto, ki je eden od primerov ribarjenja, pošiljanje osebnih in občutljivih podatkov, verižnih sporočil s seznami vseh poštnih naslovov, prijave na vprašljive spletne strani, puščanje podatkov na javnih straneh ter brezskrbnost pri preverjanju pristnosti podatkov (Šolić in sod., 2010).



Slika 2: Formalno opredeljene domene znanja in ontologije (Šolić in sod., 2013)

1.9 Varnostna politika in rešitve

Zaradi izpostavljenosti IS varnostnim tveganjem se je pojavila potreba po vzpostavitvi ustreznega sistema za upravljanje informacijske varnosti (v nadaljevanju SUIV). Zagotavljanje varnosti je kompleksna aktivnost, ki zahteva sistematičen pristop (Brezavšček in Moškon, 2010). Za ustrezno varnost sodobnih IS je potrebna obravnava vprašanj varnostne politike, ki obsegajo tehnologijo, človeško vedenje in organizacijo (Veiga in Eloff, 2010). Eden od predlogov za izboljšanje informacijske varnosti je certificiranje. Standardi ISO 27000 so najbolj učinkoviti, preverjeni in zanesljivi nabori

standardov, namenjeni vzpostavitvi informacijske varnosti in vodenju procesa upravljanja s tveganji (angl. »information security risk management«) (Bernik in Prislan 2013). Vsak IS bi moral biti podvržen natančni analizi, preden se sistem upravljanja s tveganji vzpostavi in vpelje v organizacijsko strukturo. Poznavanje organizacijskih ranljivosti, potencialnih groženj in posledic, ki bi ob njihovem uresničenju nastale, je ključnega pomena (Bernik in Prislan, 2013).

Učinkovito upravljanje informacijske varnosti zahteva kombinacijo tehničnih in procedurnih kontrol za upravljanje z informacijskim tveganjem. Vrednost nadzora je odvisna od ljudi, ki ga izvajajo in uporabljajo. Kontrole so lahko zlorabljene s strani zaposlenih, ki ne spoštujejo varnostne politike in postopkov (Kruger in Kearney, 2006). Ocena tveganja vključuje številne aktivnosti, ki lahko preizkusijo zavedanje informacijske varnosti zaposlenih v organizaciji. Vključuje fizično zaščito, preverjanje kontrol, intervjuje z zaposlenimi itn. (Landoll, 2006). Varnost pacientov na področju zdravstvene oskrbe je pomembno vprašanje. Napredek na področju IKT povečuje uporabniško dostopnost in zaščito zasebnosti, ki vključuje uporabo posebnih tehnologij. Zaščito pacientovih evidenc je mogoče doseči z izvajanjem varnostnih politik z nadzorom dostopa, z ustreznimi dovoljenji in z zagotavljanjem dodatnih varnostnih ukrepov (Win, 2005). Skrb za zagotavljanje ustreznega nivoja informacijske varnosti mora biti eden primarnih ciljev vsake organizacije, če želi zagotoviti učinkovitost izvajanja svojih procesov (Brezavšček in Moškon, 2010). Zagotavljanje ustrezne pozornosti in podpore za potrebe uporabnikov je zato treba obravnavati kot pomemben element uspešne varnostne strategije (HAISA, 2007).

2 NAMEN, HIPOTEZE IN RAZISKOVALNO VPRAŠANJE

Po pregledu literature se je izpostavilo, da so pri delu medicinskih sester prisotna vedenja, ki lahko resno ogrozijo varnost IS kot vira osebnih podatkov pacienta. Pri pregledu literature pogrešamo vir, ki bi predstavil sliko stanja omenjenih vedenj v Sloveniji. Problematičnega stanja na področju informacijske varnosti zaposlenih v zdravstveni negi v Sloveniji ni še nihče podrobno analiziral, zato smo si zastavili naslednje raziskovalno vprašanje: »Ali je znanje medicinskih sester s področja informacijske varnostni zadostno, da pri svojem delu zagotovijo celovitost in zaupnost pacientovih zdravstvenih podatkov?« Cilj naloge je torej ugotoviti, kakšno je znanje medicinskih sester na področju informacijske varnostni. Skladno s tem smo si zastavili naslednje hipoteze (H):

- H1: Potencialno tveganje omenjene populacije, povezano z uporabo računalnikov, znaša več kot 66 %.
- H2: Stopnja ozaveščenosti omenjene populacije o varnosti informacij je manjša kot 64%.
- H3: Uporabniška raven prepričanja o informacijski varnosti omenjene populacije je nižja kot 45 %.
- H4: Več kot 80 % omenjene populacije ima slabe navade pri zagotavljanju sistematičnih zamenjav vstopnih gesel.

Pri formuliranju hipotez smo se osredotočili na vrednosti iz preteklih študij omenjenega področja (Albarrak, 2011; Šolić in sod., 2014).

3 METODE DELA IN MATERIALI

V nalogi sta uporabljeni dve ključni metodi raziskovanja, in sicer pregled literature in kvantitativni raziskovalni pristop (metoda anketiranja). Podrobnosti uporabe omenjenih metod so predstavljene v nadaljevanju poglavja.

3.1 Pregled literature

V prvi fazi izdelave magistrskega dela smo relevantno znanstveno in strokovno literaturo s področja zdravstvene nege in informatike poiskali s pregledom monografij (sistem COBISS), člankov in spletnih strani. Pri iskanju so nam bile v pomoč tudi indeksirane specializirane baze podatkov: Science Direct, EBSCO host, Wiley Online Library, PubMed, CINAHL in Googlov učenjak. Uporabili smo napredno iskanje logičnega operatorja »and« z omejitvijo zadnjih 10 let in polna besedila člankov. Pri tem smo uporabili več ključnih besed in besednih zvez: zdravstvena nega (»nursing«), informacijska varnost (»information security«), varnostno vedenje (»security behaviours«) in varovanje podatkov (»data security«). Anketiranje je potekalo od 29. 4. 2015 do 31. 8. 2015. Z metodo pregleda literature, z deskriptivno metodo in metodo kompilacije smo povzeli nekatere izide že opravljenih raziskav na področju IKT v zdravstveni negi.

3.2 Postopek zbiranja podatkov

Podatke za namen raziskave smo zbirali na dva načina, in sicer s pomočjo spletne ankete v aplikaciji 1KA (en klik anketa) ter na običajen način – rutinsko zbiranje podatkov (papirnata verzija ankete). Pri iskanju sodelujočih smo naleteli na veliko neodobravanje, predvsem zavrnitev s strani Zbornice-Zveze, nekaterih strokovnih regijskih društev, bolnišnic, zdravstvenih domov in socialno - varstvenih zavodov. Od velikega števila omenjenih nismo dobili niti potrjenega niti zavrnjenega odgovora za sodelovanje. Povezava do spletne ankete je bila objavljena na spletni strani regijskega strokovnega društva medicinskih sester, babic in zdravstvenih tehnikov, nekatere so bile posredovane preko elektronske pošte in družabnih spletnih strani, ostale so bile izpolnjene ročno, kakor so po dogovoru želele določene institucije. Tako smo pridobili 135 rešenih spletnih in 39 papirnatih anket. S tem smo poskusili pridobiti čim bolj razpršen vzorec, ki naj bi predstavljal celotno populacijo medicinskih sester v Republiki Sloveniji iz različnih delovnih organizacij, vseh ravni zdravstva in socialnega varstva.

3.2.1 Vzorec

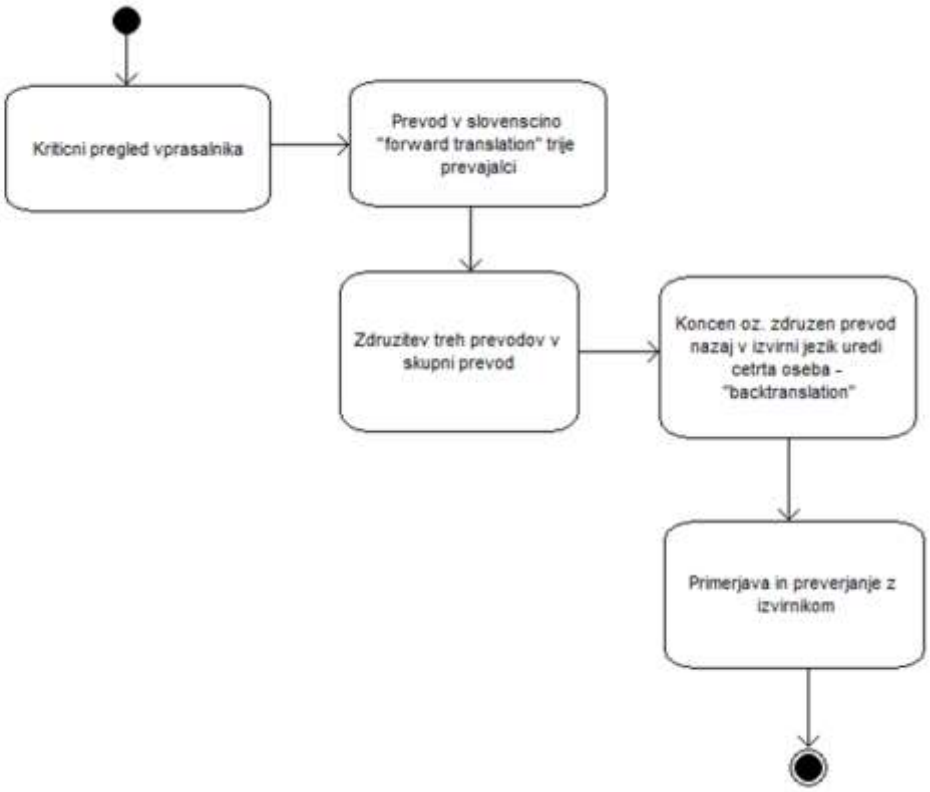
V raziskavi je sodelovalo skupaj 174 anketirancev stroke zdravstvene nege. Od tega 152 žensk (87,36 %) in 22 moških (12,64 %). Razpon starosti anketirancev je bil od 19 do 59 let. Povprečna starost je bila 37,64 let. Največji delež anketirancev je imel visokošolsko izobrazbo tj. diplomirana medicinska sestra/diplomirani zdravstvenik (45,98 %). Sledi srednješolska izobrazba - zdravstveni tehnik (40,80 %), višješolska izobrazba - višja medicinska sestra (3,45 %), magister zdravstvene nege (8,04 %) in drugo: bolničar/negovalec/itn. (1,72 %). Največ sodelujočih je imelo delovno mesto na primarni zdravstveni ravni, in sicer 38,50 %, sledijo sekundarna 22,99 % in terciarna zdravstvena raven 22,41 % ter socialno - varstveni zavod 16,09 %.

3.2.2 Vprašalnik

Za zbiranje podatkov smo uporabili anketni vprašalnik za prepoznavanje vedenja in oceno znanja informacijske varnosti, ki so ga razvili Šolić in sod. (2014). Po pregledu vprašalnika smo za dovoljenje souporabe in prevod (glej prilogo 1) prosili njegove prvotne avtorje. Enak oziroma preveden in prilagojen vprašalnik za področje zdravstvene nege smo uporabili tudi mi. S pomočjo vprašalnika UISAQ smo ugotavljali potencialno tvegano vedenje in zavedanje uporabnikov – medicinskih sester na področju varnosti IKT. Postopek prevoda je prikazan na sliki 3. Vprašalnik smo iz hrvaškega jezika v slovenščino prevedli (ang. »forward translation«) trije prevajalci (postopek prevoda povzet po Råholm, 2010). Sledila je primerjava in združitev vseh treh prevodov. Končen prevod je iz slovenščine v hrvaščino (angl. »backtranslation«) naredila četrta oseba. To verzijo smo nato primerjali z izvirnim vprašalnikom in preverili odstopanja. Končna slovenska verzija vprašalnika in zapisi prevoda so na voljo v prilogah (priloga 2 in 3).

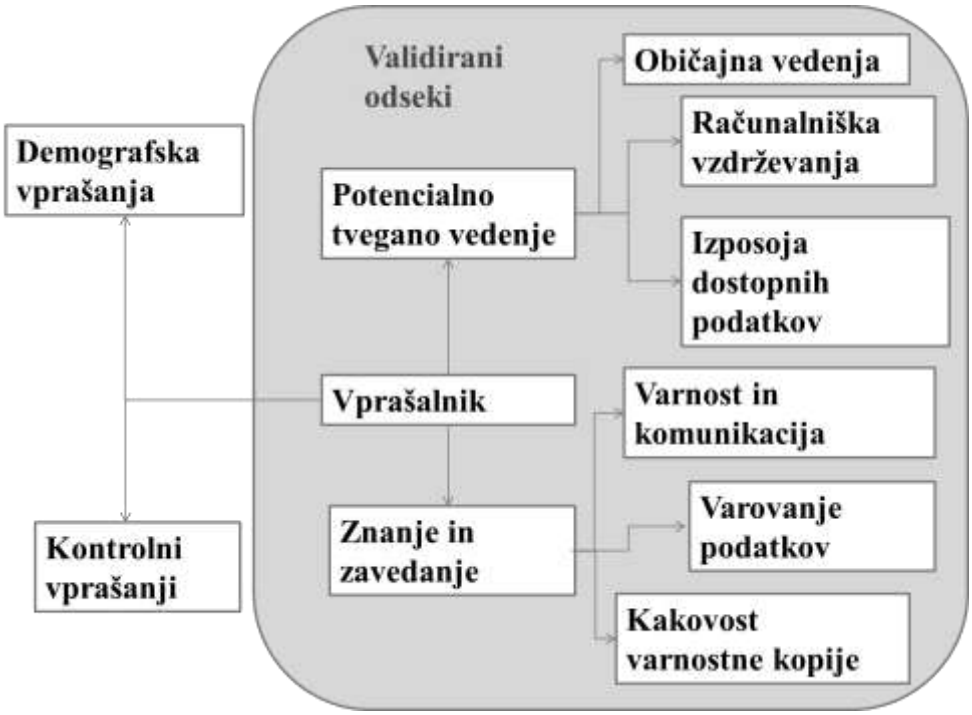
Vprašalnik je sestavljen iz odsekov, ki ugotavljajo uporabnikovo:

- potencialno tvegano vedenje,
- raven ozaveščenosti o varnosti informacij,
- raven prepričanj o informacijski varnosti in
- varovanje gesel.



Slika 3: Postopek prevoda

Prvi sklop vprašanj se nanaša na demografske podatke: spol, starost, najvišja dosežena formalna izobrazba, delovno mesto in uporaba dostopnih podatkov do računalnika doma ter v službi. Sledijo vprašanja o potencialno tveganem vedenju (običajna vedenja, računalniška vzdrževanja in izposoja dostopnih podatkov), o znanju zavedanju (varnost in komunikacija, varovanje podatkov in kakovost varnostnih kopij). Anketiranci so odgovarjali na ponujene trditve in označili tiste, ki najbolj držijo zanje. Struktura vprašalnika je predstavljena na sliki 4.



Slika 4: Struktura vprašalnika

3.2.3 Analiza podatkov

Za obdelavo podatkov in statistično analizo smo uporabili program Microsoft Office Excel 2010 in IBM SPSS 20.

4 REZULTATI

V nadaljevanju naloge so v podpoglavjih predstavljeni pridobljeni rezultati potencialnega tveganega vedenja, ravni ozaveščenosti o varnosti informacij, ravni prepričanja o informacijski varnosti ter varnosti gesel.

4.1 Rezultati potencialno tveganega vedenja

4.1.1 Običajna vedenja

Od skupaj 174 anketirancev jih je na vprašanje o uporabi avtentikacijskih podatkov (uporabniško geslo) za dostop do službenega in domačega računalnika odgovorilo 162 oz. 93,10 % vseh sodelujočih. Pridobljeni odgovori so bili zanimivi, saj so anketiranci odgovorili, da na delu uporabljajo dostopne podatke v 94,25 % primerov, doma pa le v 63,79 %.

4.1.2 Izposoja dostopnih podatkov

Uporabniškega imena in gesla za dostop do računalnika 64,81 % anketirancev nikoli ne posoja sodelavcem v službi, 22,84 % jih to naredi redko, 7,41 % le nekajkrat na mesec, nekajkrat na teden 3,09 %, skoraj vsak dan pa 1,85 % anketiranih. Podobne rezultate smo dobili tudi pri vprašanju o posojanju dostopnih podatkov prijateljem, sorodnikom in znancem. Kar 70,37 % anketiranih dostopnih podatkov nikoli ne posoja, 19,75 % redko, 5,56 % včasih, 1,85 % pogosto in 2,47 % vsak dan.

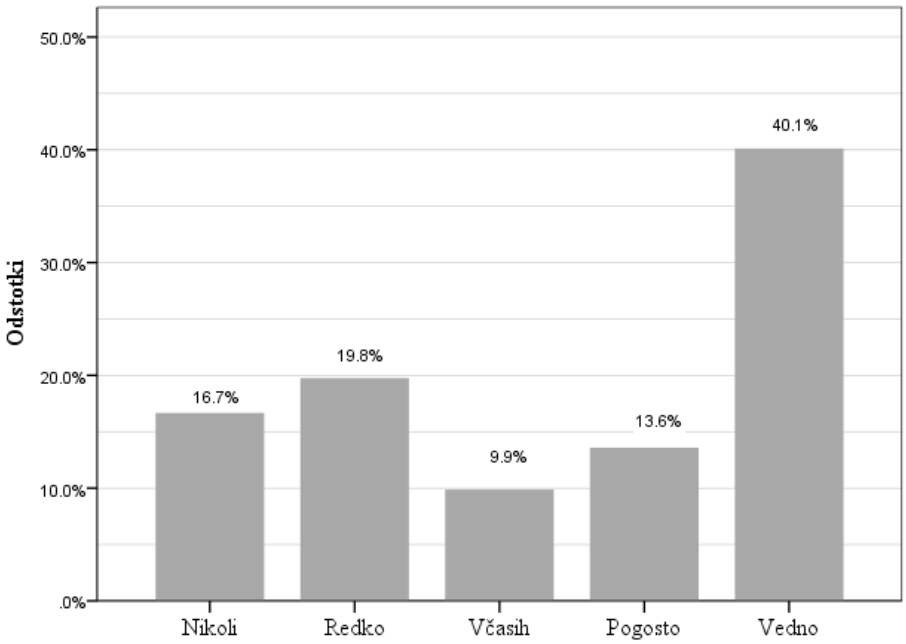
Preverili smo, ali obstaja povezava med pogostostjo posojanja dostopnih podatkov do računalnika drugim in starostjo anketirancev. Identificirali smo statistično pomembno šibko negativno korelacijo med omenjeno pogostostjo posojanja in starostjo ($r = -0,323$; $p<0,001$). Slednje pomeni, da mlajši anketiranci pogosteje posojajo svoja gesla za dostop do domačega računalnika drugim, medtem ko starejši to počnejo redkeje. Podobna izredno šibka negativna korelacija s starostjo se je pokazala tudi za posojanje gesel sodelavcem ($r = -0,175$; $p = 0,027$).

Uporabniško ime in geslo za dostop oz. prijavo v osebno elektronsko pošto nikoli ne posoja prijateljem, sorodnikom in znancem 80,25 % anketiranih, 15,43 % jih posoja redko (nekajkrat na leto), včasih 1,86 %, pogosto 1,23 % in vedno 1,23 %.

Od skupaj 174 je na naslednje vprašanje odgovorilo 162 anketirancev oz. 93,10 % vseh sodelujočih. Največji delež anketirancev tj. 98,14 % nikoli z glasno izgovorjavo ne razkriva svoje PIN kode (angl. »Personal Identification Number«) prodajalcu, ko plačuje s plačilno kartico v trgovini. 0,62 % to počne redko, 0,62 % včasih, vedno pa 0,62 %. Redko tj. 11,73 % anketirancev posoja svoje plačilne kartice in PIN kodo prijateljem, sorodnikom in znancem, medtem ko jih 84,57 % tega nikoli ne počne. Včasih (mesečno) to počne 1,85 %, tedensko 0,62 %, skoraj vedno pa 1,23 %.

Od skupaj 174 je na naslednje vprašanje odgovorilo 162 anketirancev oz. 93,10 % vseh sodelujočih. Za različne IKT sisteme (npr. Facebook, elektronska pošta, poslovni računi) jih 16,67 % nikoli ne uporablja različna vstopna gesla. Različna vstopna gesla

uporablja redko 19,75 %, včasih pa 9,88 % anketiranih. Tako jih pogosto uporablja 13,58 % in vedno 40,12 % različna gesla za posamezne IKT sisteme (slika 5).



Slika 5: Porazdelitev odgovorov na trditev »Za različne informacijsko komunikacijske sisteme (Facebook, elektronska pošta, poslovni računi) uporabljam različna vstopna gesla«

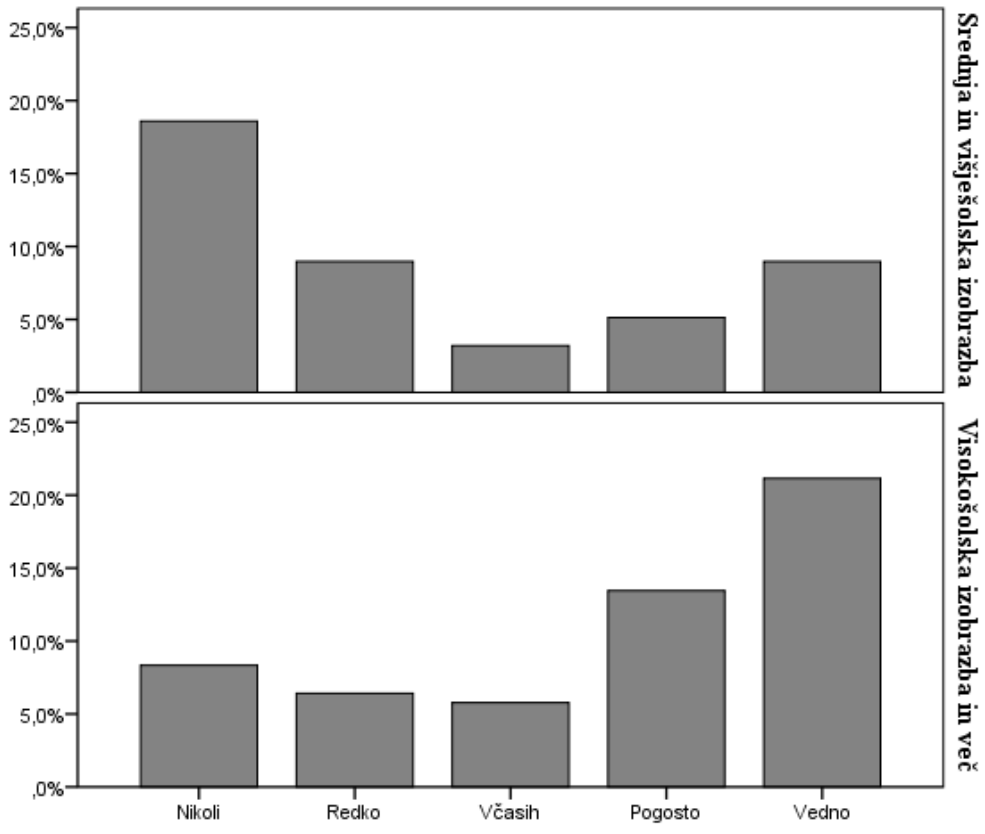
4.1.3 Vzdrževanje

Od skupaj 174 je na naslednje vprašanje odgovorilo 157 anketirancev oz. 90,23 % vseh sodelujočih. Manj kot četrtina anketirancev – 26,11 % pogosto (nekajkrat na teden) vzdržuje zaščito svojega osebnega računalnika z rednimi posodobitvami, antispyware in antivirusnimi programi, 24,21 % jih to počne vedno, redko 22,93 % in včasih 22,29 %. Samo 4,46 % anketirancev tega nikoli ne počne. Manj kot četrtina anketirancev – 26,11 % pogosto vzdržuje nadgradnjo vseh uporabniških programov in operacijskega sistema na osebnem računalniku. Tega nikoli ne počne 4,46 % anketirancev, redko 28,66 %, včasih 22,93 % in vedno 17,84 % anketirancev. Na svoj osebni računalnik nameša zanimive, ne pa nujno potrebne programe neznanih ali manj znanih avtorjev redko (nekajkrat na leto) 40,13 % anketirancev, včasih (nekajkrat na mesec) 12,10 %, nikoli 42,04 %, pogosto 4,46 % in vedno 1,27 %. Dodatno smo preverili, ali obstaja povezava med pogostostjo nameščanja programov in starostjo anketirancev. Ugotovili smo statistično pomembne šibke negativne korelacije ($r = -0{,}321$; $p < 0{,}001$), kar pomeni, da mlajši anketiranci pogosteje nameščajo manj pomembne programe kakor starejši.

Od skupaj 174 je na naslednje vprašanje odgovorilo 157 anketirancev oz. 90,23 % vseh sodelujočih. Svojih osebnih podatkov (npr. osebni naslov, št. telefona, razna obvestila) nikoli ne objavlja na družabnih omrežjih 82,16 % anketirancev, 13,38 % jih to počne redko, vedno 0,64 %, pogosto 1,27 % in včasih 2,55 %. Preverili smo povezavo med pogostostjo objave podatkov na spletnih straneh in starostjo anketirancev. Identificirana je bila statistično pomembna šibka in negativna korelacija med omenjenima

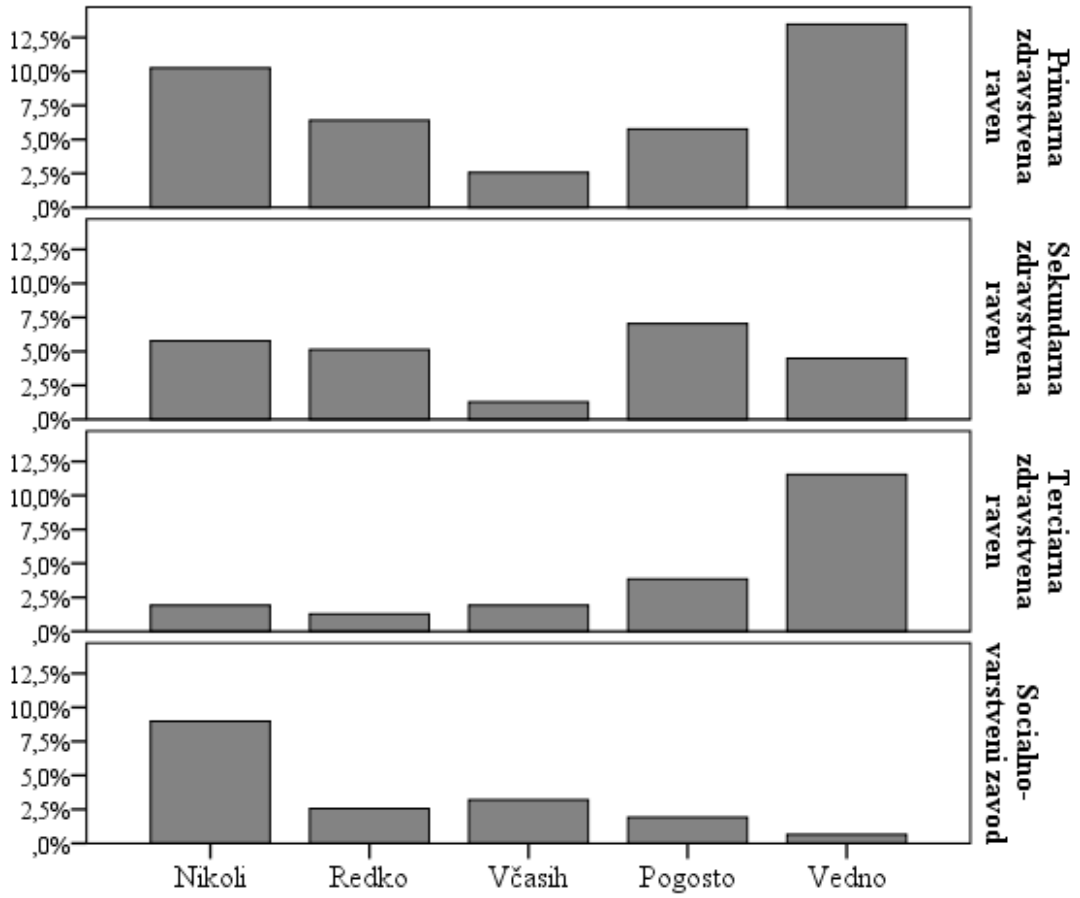
spremenljivkama (r = - 0,344; p < 0,001). Slednje pomeni, da mlajši anketiranci pogosteje objavljajo podatke na svetovnem spletu (npr. na družabnih omrežjih itn.) kot starejši. Od skupaj 174 je na naslednje vprašanje odgovorilo 157 anketirancev oz. 90,23 % vseh sodelujočih. Na trditev o odpiranju in odgovarjanju na elektronsko pošto neznanih/sumljivih pošiljateljev jih 85,99 % tega nikoli ne počne, redko 11,46 %. Včasih to počne 1,91 % in vedno 0,64 % anketirancev.

Od skupaj 174 je na naslednja vprašanja odgovorilo 156 anketirancev oz. 89,65 % vseh sodelujočih. Elektronsko pošto neznanih pošiljateljev odpira brez preverjanje prilog 19,23 % redko, včasih 4,49 %, vedno 2,56 %, pogosto 0,64 % in nikoli 73,08 %. Verižno elektronsko pošto pošilja/posreduje redko (nekajkrat na leto) 26,28 % anketiranih, včasih (nekajkrat na mesec) 6,41 %, nikoli pa jih ne pošilja 64,74 %. Pogosto to počne 1,93 % in vedno 0,64 % anketirancev. Več elektronskih naslovov (npr. osebno in službeno) uporablja vedno 30,13 % anketiranih, nikoli 26,92 %, redko 15,39 %, včasih 8,97 % in pogosto 18,59 % anketirancev. Preverili smo, ali je število uporabljenih različnih elektronskih naslovov povezano s stopnjo izobrazbe. S pomočjo Mann Whitneyevega U testa smo identificirali statistično pomembne (U=1891,0; z = - 4,11; p < 0,001) razlike med tistimi anketiranci z nižjo izobrazbo (srednja in višješolska) in višjo izobrazbo (visoka in univerzitetna), ki so prikazane tudi na sliki 6.



Slika 6: Razlike v porazdelitvi odgovorov na trditev »Uporabljam več elektronskih naslovov (npr. osebno in službeno elektronsko pošto).«

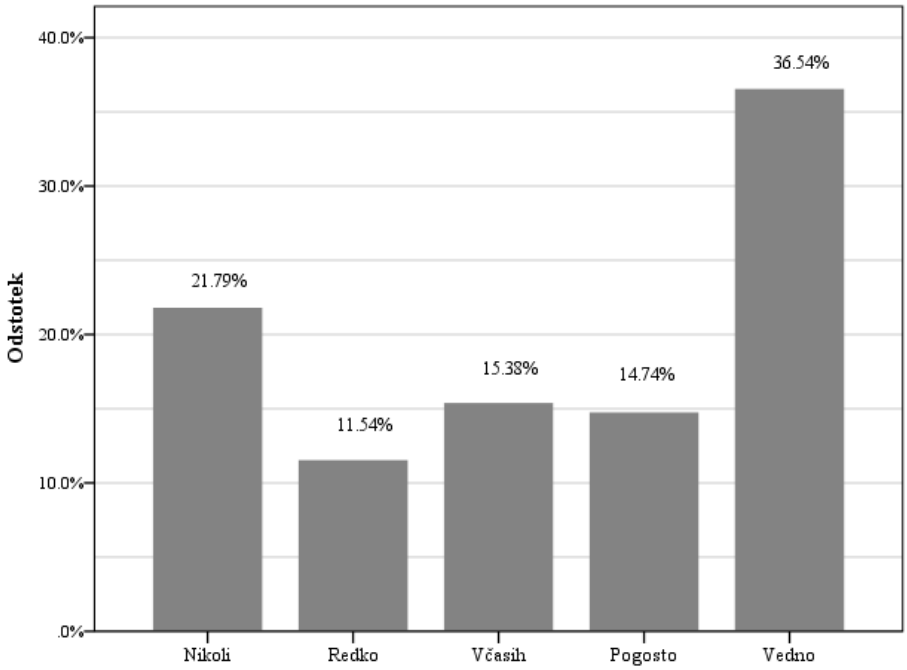
Kot zanimivost smo preverili, ali pri anketirancih obstajajo razlike pri številu uporabljenih elektronskih naslovov (npr. osebna in službena elektronska pošta) glede na zaposlitev v primarni, sekundarni, terciarni zdravstvei ravni in socialnih varstvenih zavodih. Slika 7 kaže, da najpogosteje uporabljajo več elektronskih naslovov v primarni in terciarni ravni zdravstvenega varstva, medtem ko v socialno - varstvenih zavodih največ zaposlenih nikoli ne uporablja več elektronskih naslovov. S pomočjo χ^2 preizkusom smo ugotovili, da so opisane razlike med skupinami statistično pomembne ($\chi^2 = 9{,}884$, df = 2, p = 0,007).



Slika 7: Porazdelitev odgovorov na trditev: »Uporabljam več elektronskih naslovov« glede na zaposlitev v primarnem, sekundarnem, terciarnem zdravstvu varstvu in socialnih - varstvenih zavodih

Nikoli - 36,54 % se v elektronsko pošto ne prijavlja iz različnih javnih spletnih mest (npr. spletna kavarna, razne ustanove z uporabo brezplačne povezave). Letno – jo uporablja 34,62 %, nekajkrat na mesec - včasih 17,95 %, nekajkrat na teden – pogosto 8,33 % in vedno 2,56 % anketirancev. Poleg tega smo preverili, ali obstaja povezava med pošiljanjem elektronske pošte z javnih spletnih mest in starostjo anketirancev. Identificirali smo statistično pomembne šibke in negativne povezave ($r = -0{,}344$; $p < 0{,}001$). Preverili smo tudi razlike glede na stopnjo izobrazbe. Ugotovili smo statistično pomembne razlike ($U = 2339$; $z = -2{,}515$; $p = 0{,}012$) med stopnjo izobrazbe anketirancev in prijavljanje v elektronsko pošto iz različnih javnih spletnih mest.
Od skupaj 174 je na naslednje vprašanje odgovorilo 156 anketirancev oz. 89,65 % vseh sodelujočih. Po delu se iz informacijskega sistema vedno odjavi 82,05 % anketirancev,

pogosto 7,69 %, včasih 1,92 %, redko 5,24 % in nikoli 5,13 %. Svoj računalnik zaklene, ko na kratko odide iz pisarne, od delovne mize na stranišče ali odmor le 36,54 % anketirancev. Redko jih to naredi 11,54 %, včasih 15,38 %, pogosto 14,74 %, nikoli pa 21,79 % (slika 8).



Slika 8: Porazdelitev odgovorov na trditev »Računalnik zaklenem, ko na kratko odidem iz pisarne, od delovne mize, na stranišče ali odmor«

4.2 Rezultati, ki se nanašajo na znanje in zavedanje za posamezna podpodročja varnosti

4.2.1 Varnost in komunikacija

Od skupaj 174 je na naslednja vprašanja odgovorilo 153 anketirancev tj. 87,93 % vseh sodelujočih. Na zastavljeno vprašanje o varnosti dopisovanja preko elektronske pošte so anketiranci odgovorili, da je ta način komuniciranja popolnoma nevaren v 1,96 %. Kot razmeroma nevarno se jih je opredelilo 23,53 %. Za odgovor »ne vem« se je odločilo 18,30 %, razmeroma varno 50,98 % in popolnoma varno 5,23 %. Komunikacija preko svetovnega spleta (npr. s pomočjo Skypa, Vibra, klepetalnice) se je z najvišjim deležem, tj. 37,91 % izkazala kot razmeroma nevarna, sledi ji razmeroma varna s 30,72 %, »ne vem« z 22,88 %, popolnoma nevarna 7,84 % in popolnoma varna z 0,65 %. Preverili smo, ali obstaja povezava o varnosti dopisovanja preko elektronske pošte in starostjo anketiranih. Dobili smo statistično pomembne šibke – negativne povezave ($r = - 0,261$; $p = 0,001$). Rezultati nakazujejo, da so mlajši anketiranci bolj prepričani v varnost dopisovanja preko elektronske pošte.

Komunikacijo preko družabnih omrežij so označili kot popolnoma nevarno s 17,65 %, razmeroma nevarno s 43,79 %, »ne vem« 16,34 % in razmeroma varno 22,22 %. Komunikacijo preko mobilnega telefona (pogovor, sporočila) so anketiranci označili kot popolnoma nevarno 4,57 %, razmeroma nevarno 25,49 %, »ne vem« 13,73 %, razmeroma varno 51,63 % in popolnoma varno 4,58 %. Korelacija med nevarnostjo

komunikacije preko mobilnega telefona in starostjo anketiranih je statistično pomembna – šibka in negativna (r = - 0,231, p = 0,004).

Rezultati kažejo, da mlajši opredeljujejo komunikacijo prek mobilnega telefona kot nevarno pogosteje kakor starejši. Pri komunikaciji preko stacionarnega telefona anketiranci menijo, da je ta komunikacija popolnoma nevarna v 3,27 %, razmeroma nevarna z 22,22 %, ne vem 11,11 %, razmeroma varna 57,52 % in popolnoma varna s 5,88 %.

4.2.2 Varovanje podatkov

Od skupaj 174 je na naslednja vprašanja odgovorilo 153 anketirancev oz. 87,93 % vseh sodelujočih. Na vprašanje o prepričanju kraje službenih podatkov s službenega računalnika (v organizaciji, kjer delajo) je 28,10 % anketirancev navedlo, da niso prepričani v celoti. Za mogoč scenarij se je opredelilo 37,26 % anketirancev, za »ne vem« pa 21,57 %. V krajo je deloma prepričanih 9,80 % in popolnoma prepričanih 3,27 %. Pri kraji podatkov z osebnega računalnika 26,80 % anketirancev ni bilo prepričanih v celoti, popolnoma prepričanih je 1,96 %, delno pa 9,15 %. Odgovor »ne vem« je izbralo 15,69 %, kot možen scenarij pa 46,40 %.

V krajo podatkov z mobilnega telefona je deloma prepričanih 9,80 %, popolnoma 2,62 % anketirancev, 25,49 % pa ni prepričanih v celoti. Odgovor »ne vem« je izbralo 16,34 %, kot možen dogodek pa 45,75 % anketiranih. V možnost odtujitve denarja s tekočega računa je popolnoma prepričanih 5,23 %, deloma pa 11,76 % anketiranih. 27,45 % ni prepričanih v celoti, mogoče 41,18 % in »ne vem« 14,38 %. V krajo identitete na svetovnem spletu (npr. preko e-banke, Facebooka, elektronske pošte) je popolnoma prepričanih 3,92 %, deloma 14,38 %, »ne vem« 20,26 %, mogoče 35,9 5% in 25,49 % anketirancev ni prepričanih v celoti.

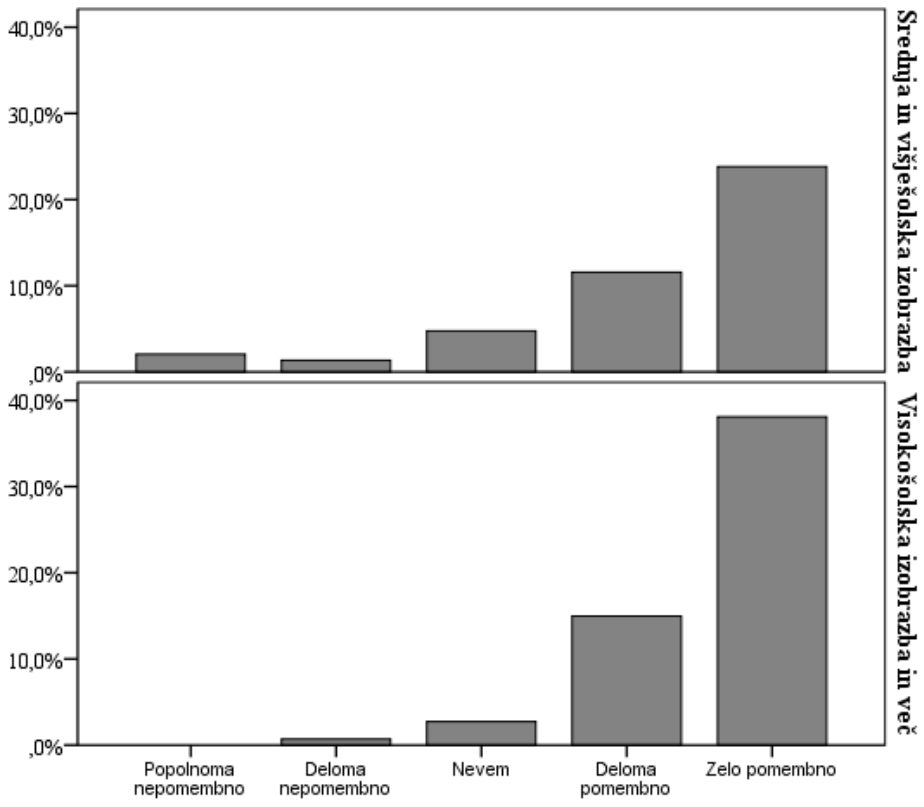
4.2.3 Kakovost varnostne kopije

Od skupaj 174 je na naslednja vprašanja odgovorilo 147 anketirancev oz. 84,48 %. Pri vprašanju o shranjevanju dokumentov še na dodatno lokacijo ali spominsko enoto (izdelava varnostnih kopijo podatkov) smo dobili sledeče rezultate: največji delež, tj. 65,99 % je izdelavo varnostnih kopij označilo kot zelo pomembno, 18,37 % pa kot deloma pomembno. Le 2,04 % sodelujočih je označilo kot popolnoma nepomembno. Kot deloma nepomembno jo je označilo 4,76 % in 8,84 % anketirancev je izbralo odgovor »ne vem«.

Zanimalo nas je, ali se shranjevanje pomembnih dokumentov na dodatne spominske enote (varnostna kopija) razlikuje glede na stopnjo izobrazbe anketiranih. Ugotovili smo statistično pomembne razlike (U = 2090; z = - 2,632; p = 0,008) med stopnjo izobrazbe anketirancev in shranjevanjem dokumentov na dodatno lokacijo. Rezultati so pokazali izredno nizke pozitivne, statistično pomembne povezave (r = 0,218; p = 0,008), ki nakazujejo, da nižje izobraženi anketiranci redkeje shranjujejo podatke na dodatne lokacije, medtem ko višje izobraženi to počnejo pogosteje.

Kot zelo pomembno je 69,39 % anketirancev označilo preverbo tujega medija (npr. USB ključek) pred uporabo, ali je okužen z virusi. Kot deloma pomembno je označilo 19,05 % anketirancev, popolnoma in deloma nepomembno pa 2,04 %. Le 7,48 % anketirancev je bilo neodločenih. Preverili smo povezavo med preverbo tujega medija in starostjo anketiranih. Izračunali smo statistično pomembno, vendar neznatno pozitivno korelacijo (r = 0,185, p = 0,027).

Od skupaj 174 je na naslednji vprašanji odgovorilo 147 anketirancev oz. 84,48 %. Brezpogojno varovanje gesel je večina anketirancev (82,99 %) označila kot zelo pomembno, kot deloma pomembno s 13,61 %, »ne vem« 2,04 %, deloma nepomembno 0,68 % in popolnoma nepomembno 0,68 %. Kot zelo pomembno so označili periodično zamenjavo gesel za pomembnejše sisteme z 61,91 %, kot deloma pomembno 26,53 %, kot popolnoma nepomembno 2,04 %, deloma nepomembno 2,04 %. Neodločenih je bilo 7,48 % anketirancev. Zanimalo nas je ali se periodična zamenjava gesel za pomembnejše sisteme razlikuje glede na stopnjo izobrazbe anketiranih. Identificirali smo stastistično pomembne razlike (U = 2219,000; z = -1,980; p = 0,048) glede na stopnjo izobrazbe in periodične zamenjave gesel. Rezultati kažejo, da nižje izobraženi redkeje vršijo periodično zamenjavo gesel kot visoko in več izobraženi (slika 9).



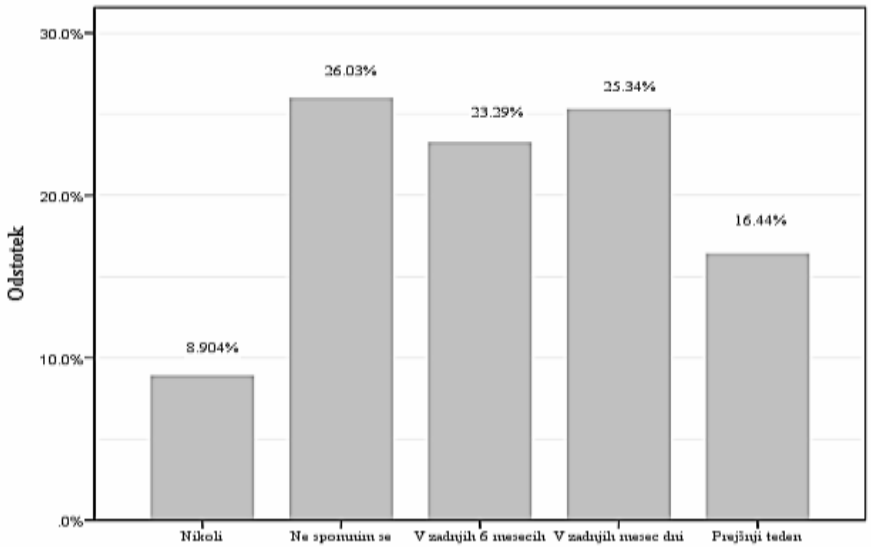
Slika 9: Porazdelitev odgovorov, ki se nanašajo na pomembnost periodične menjave gesel gleda na stopnjo izobrazbe

Od skupaj 174 je na naslednji vprašanji odgovorilo 147 anketirancev oz. 84,48 % vseh sodelujočih. Zelo pomemben element zaščite je ločevanje poslovnih računalniških virov od osebnih (npr. osebni prenosni disk, elektronska pošta, telefon).

Večina anketirancev, tj. 66,67 % je zgornjo trditev ovrednotila kot zelo pomembno, 24,49 % deloma pomembno, deloma nepomembno 0,68 % in popolnoma nepomembno 1,36 %. Neodločenih je bilo 6,80 % anketiranih.

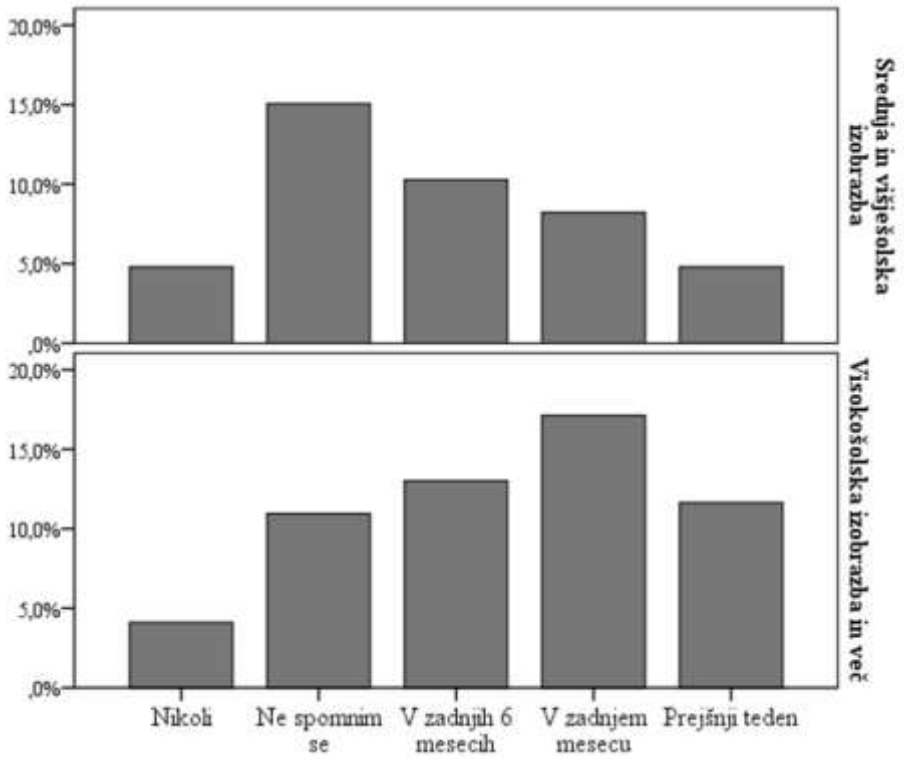
Varovati pred krajo svoj USB disk oz. USB ključek s pomembnimi podatki je kot zelo pomembno označilo kar 82,31 % anketirancev, kot deloma pomembno pa 14,29 %. Neodločenih je bilo 3,40 %. Od skupaj 174 je na naslednji vprašanji odgovorilo 146 anketirancev oz. 83,91 % vseh sodelujočih.

Pri vprašanju o izdelavi zadnje varnostne kopije podatkov so anketiranci odgovorili sledeče: 26,03 % se jih ne spomni, kdaj so zadnjič naredili kopijo; 23,29 % je kopijo podatkov naredilo v zadnjih 6 mesecih; 25,34 % v zadnjem mesecu; 16,44 % prejšnji teden, medtem ko 8,90 % kopije ni naredilo nikoli (slika 10).



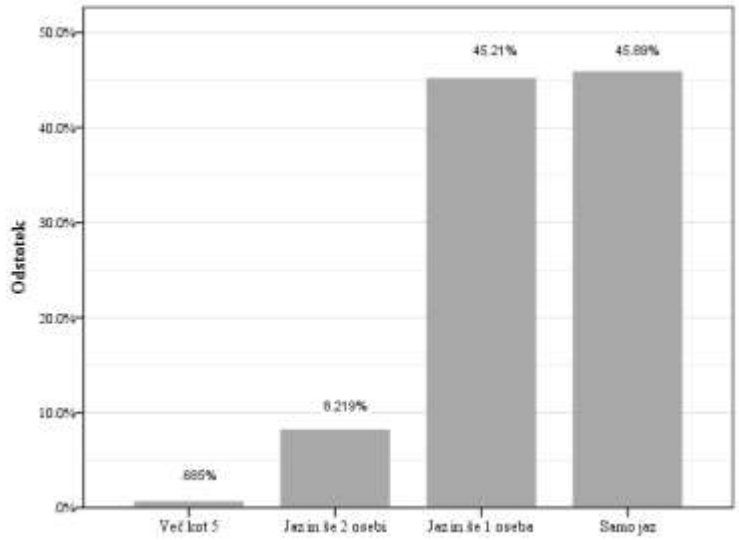
Slika 10: Porazdelitev odgovorov na trditev »Kdaj ste zadnjič naredili varnostno kopijo (angl. »backup«) osebnih podatkov ali dokumentov?«

Preverili smo še, ali se izdelava varnostnih kopij osebnih podatkov in dokumentov razlikuje glede na stopnjo izobrazbe anketiranih. Izračunali smo statistično pomembne razlike (U= 1965,000; z = - 2,635; p = 0,008) glede na stopnjo izobrazbe medicinskih sester in pogostostjo izdelave varnostnih kopij. Rezultati nakazujejo, da bolj izobražene medicinske sestre pogosteje izdelujejo varnostne kopije dokumentov (slika 11).



Slika 11: Pogostost izdelave varnostnih kopij glede na stopnjo izobrazbe

Od skupaj 174 je na naslednji vprašanji odgovorilo 146 anketirancev, oz. 83,91 %. Največ anketirancev 45,89 % je odgovorilo, da poznajo geslo za dostop do svoje elektronske pošte le oni; 45,21 % navaja, da geslo poleg njih pozna še ena oseba; 8,22 % navaja, da geslo poleg njih poznata še dve osebi; 0,68 % pa si deli geslo z več kot petimi osebami (slika 12).



Slika 12: Porazdelitev odgovorov na trditev » Koliko oseb pozna geslo za pristop v Vašo elektronsko pošto?

5 RAZPRAVA

Analiza odgovorov je pokazala zanimive rezultate, ki so v določenih primerih primerljivi z ugotovitvami ostalih avtorjev. Cilj naloge je bil ugotoviti, kakšno je znanje medicinskih sester s področja informacijske varnosti. Skladno s tem smo v nadaljevanju s pomočjo rezultatov potrdili in ovrgli hipoteze ter odgovorili na raziskovalno vprašanje, ki smo si ga postavili na začetku naloge. Skladno s spodnjim opisom rezultatov zavrnemo prvo hipotezo (H1): »Potencialno tveganje omenjene populacije povezano z uporabo računalnikov znaša več kot 66 %.« Računalnik zaklene, ko na kratko odide iz pisarne, od delovne mize na stranišče ali odmor le 36,54 % anketirancev, nikoli pa 21,79 %. Glede na možnosti vdora in kraje podatkov preko elektronskih virov je toleranca informacijske varnosti, predvsem v ustanovah, kjer predstavlja varovanje osebnih podatkov, ključnega pomena.

Villanueva in sodelavci (2011) so v svoji raziskavi opredelili, da večina medicinskih sester, zajetih v raziskavo, tj. 76,70 %, uporablja internet pri svojem vsakdanjem delu. Skoraj tretjina, tj. 28,9 % jih na delovnem mestu dostopa do interneta vsak dan. Skladno z rezultati so identificirali dva profila medicinskih sester – uporabnikov IKT ter tako razdelili stroko na dva profila uporabnikov, ki predstavljata medicinske sestre (4,58 %), ki IKT pripisujejo dodatno vrednost in jo smatrajo kot sestavni del prakse, ter »neintegrirane medicinske sestre« (95,42 %), ki IKT ne pripisujejo pomembnosti (Villanueva in sod., 2011). Tudi Furnell in sodelavci (2006) so ocenili razumevanje 340 uporabnikov varnostnih funkcij v nekaterih aplikacijah (npr. Internet Explorer, Outlook Express in Microsoft Word), ki omogočajo izbiro in konfiguracijo, pri tem pa morajo uporabniki sprejeti odločitve povezane z varnostjo (Furnell in sod., 2006). V drugi raziskavi so Aleman in sodelavci (2014) analizirali uporabo IKT in družabnih omrežij med visokošolskimi učitelji in sodelavci univerz zdravstvene nege v Španiji. Vzorec je zajel 165 predavateljev iz 25 fakultet. Pri svojem delu le 71 % predavateljev uporablja internet, največkrat (63 %) za iskanje informacij, 72 % za pošiljanje elektronske pošte in sistema za e-izobraževanje Moodle. Kljub temu, da je 51 % visokošolskih učiteljev imelo na svojih urah več kot 120 študentov, se je izkazalo, da samo število študentov ni odločilni dejavnik, ki bi pripomogel k temu, da bi visokošolski učitelji imeli večji interes za izboljšanje svojega znanja na področju IKT. Pri mlajši generaciji iz omenjene skupine je bilo uporabljenih več sodobnih IKT (Aleman in sod., 2014).

V naši raziskavi 26,11 % anketirancev opravi zaščito svojega osebnega računalnika s posodobitvami protivohunskih in protivirusnih zaščit pogosto (nekajkrat na teden), 24,21 % pa vedno. Redko jih to počne 22,93 % in včasih 22,29 %. 26,11 % pogosto vzdržuje nadgradnjo vseh uporabniških programov in operacijskega sistema na osebnem računalniku. Tega nikoli ne počne 4,46 % anketirancev. Na svoj osebni računalnik namešča zanimive, ne pa nujno potrebne programe neznanih ali manj znanih avtorjev redko (nekajkrat na leto) 40,13 % anketirancev, nikoli 42,04 %. Študija, ki so jo izvedli na Japonskem, je v raziskavo zajela medicinske sestre 515 naključno izbranih bolnišnic, v katerih je bilo uvedeno e-naročanje (Nimi in Ota, 2014). Omenjena študija je pokazala, da nekatere bolnišnice sledijo različnim varnostnim ukrepom, vendar določene medicinske sestre niso prepoznale varnostnih vzdrževalnih ukrepov. Nekoliko manj kot polovica (40 %) meni, da bi moral biti obseg delitev informacij omejen v okviru vsake poklicne skupine. Pri identifikaciji za uporabo elektronskih zdravstvenih zapisov večina uporablja geslo in osebno izkaznico (angl. »ID – Identity Card), manj

kot 10 % jih uporablja identifikacijsko kodo/oznako (angl. »IC – Identity Code«) ali prstni odtis. Glede varnostnih ukrepov, ki so bili dejansko sprejeti v ustanovah, so medicinske sestre navedle redno obnavljanje gesel (58,1 %), sledi ohranjevalnik zaslona in prisilna odjava (54 %).

Raziskava, ki je za zbiranje podatkov uporabila UISAQ vprašalnik, je pokazala, da 28,8 % uporabnikov razkriva svoja gesla za dostop do službene elektronske pošte (Šolić, Veliki, Galba, 2015). Rezultati naše raziskave kažejo, da 94,25 % medicinskih sester za dostop do službenega računalnika uporablja uporabniško ime in geslo, medtem ko na domačih računalnikih to počne samo 63,79 %. Večina, tj. 64,81 % anketirancev nikoli ne posoja teh podatkov sodelavcem v službi, 22,84 % jih to naredi redko. Doma, sorodnikom in znancem teh podatkov nikoli ne posoja 70,37 %, redko jih to naredi 19,75 %. Po delu se v službi iz informacijskega sistema vedno odjavi 82,05 % anketirancev. Svoj računalnik zaklene, ko na kratko odide iz pisarne, od delovne mize na stranišče ali odmor le 36,54 % anketirancev, nikoli pa 21,79 %.

Informacijski pooblaščenec zahteva uporabo posameznih dostopnih pravic (uporabniška gesla) in prijavo uporabnika v sistem pred delom ter odjavo po končanem delu, kjer odjavljanje enega in prijavljanje drugega uporabnika ne predstavlja resnejših posledic, temveč s strani uporabnika predstavlja »nadležno« in manj praktično opravilo. Po določenem času neaktivnosti uporabnika mora sistem omogočati samodejno ali ročno zaklepanje delovne postaje s strani uporabnika. Delovna postaja ne sme ostati odklenjena - dosegljiva, zlasti če je uporabnik prijavljen v IS in aplikacije in ni fizično prisoten, saj je tako odprta pot za zlorabo osebnih podatkov. Kjer zaradi narave dela (urgenca) ni smiselna uporaba posameznih dostopnih pravic, se izjemoma lahko uporabijo skupinske dostopne pravice. Razlog mora biti utemeljen, resnost in tveganje pa morata pretehtati zmožnosti natančnega ugotavljanja odgovornosti zlorabe OP. Zgolj nepraktičnost ni zadosten razlog za uporabo dostopnih pravic na ravni skupine (Informacijski pooblaščenec v sodelovanju s skupino za bolnišnične informacijske sisteme pri združenju zdravstvenih zavodov Slovenije, str. 8).

Različne oblike IKT so lahko sredstvo zagotavljanja varnosti, lahko pa so tudi območje potencialnih groženj (Svete in Pintarič, 2008, str. 76). Internet je znan vir škodljive programske opreme. Nezavarovane prenosne naprave (npr. pametni telefoni, prenosni računalniki, dlančniki), ki imajo dostop do zdravstvenega IS predstavljajo varnostno grožnjo (Šolić in Ilakovac, 2009). Računalniške viruse, ki lahko onesposobijo delovanje e-pošte in računalniškega omrežja, so v preteklosti uporabnikom dostavili v obliki elektronskega sporočila. Zlonamerne kode dosežejo omrežja v priponkah in se lahko aktivirajo tudi samodejno, brez posredovanja uporabnika (Verdonik in Bratuša, 2005, str. 130). Bratuša (2007) navaja, da se uporabniki zavedajo nevarnosti, ne vedo pa, kako se zavarovati. Uporabniki pogosto ne poznajo delovanja antivirusnih programov in požarnih zidov. Omenjeni prispevajo le toliko, kolikor je varnostno osveščen njihov uporabnik (Bratuša, 2007).

Na vprašanje o varnosti dopisovanja preko elektronske pošte je pri naši raziskavi 50,98 % anketirancev mnenja, da je omenjeni način komunikacije razmeroma varen, po drugi strani pa jih kar 23,53 % meni, da je ta način dopisovanja razmeroma nevaren. Komunikacijo preko družabnih omrežij je večina anketirancev s 43,79 % označila kot razmeroma nevarno, preko mobilnega telefona (pogovor, sporočila) z 51,63 % kot razmeroma varno, preko stacionarnega telefona so s 57,52 % anketiranci podobnega

mnenja kot pri mobilni komunikaciji. Storitev imajo za razmeroma varno. Pri komunikaciji preko svetovnega spleta so si mnenja anketirancev najbolj različna. Najvišji delež predstavlja s 37,91 % razmeroma nevarna komunikacija, sledi pa ji razmeroma varna s 30,72 %. Svojih osebnih podatkov (npr. osebni naslov, št. telefona, razna obvestila) na družabnih omrežjih ne objavlja 82,16 % anketiranih medicinskih sester. Redko jih to počne 13,38 %, včasih pa 2,55 %. Kar 85,99 % anketiranih medicinskih sester nikoli ne odpira in odgovarja na elektronsko pošto neznanih/sumljivih pošiljateljev. Redko jih to počne 11,46 %. Elektronsko pošto neznanih pošiljateljev odpira brez preverjanje prilog 19,23 % medicinskih sester, redko oz. včasih 4,49 % in nikoli 73,08 %. Verižno elektronsko pošto pošilja/posreduje redko (nekajkrat na leto) 26,28 % anketiranih, včasih (nekajkrat na mesec) 6,41 %, nikoli pa 64,74 %. Več elektronskih naslovov (npr. osebnega in službenega) uporablja vedno 30,13 % anketiranih, nikoli 26,92 %, pogosto 18,59 % anketirancev.

Šolić in Ilakovac (2009) sta v svojo pilotno študijo vključila dve skupini raziskovalcev in pedagoških delavcev iz različnih okolij, uporabnikov prenosnih računalnikov. Namen študije je bil primerjati znanja o grožnjah varnosti in navadah, ki zadevajo računalniško varnost. Dostop do internetnih storitev, kot sta uporaba spletnega bančništva ali e-pošte preko javnih računalnikov z vprašljivo zaščito, je resna grožnja podatkom. Večina udeležencev je uporabljala takšen dostop izjemoma oziroma redko, kar kaže na zavedanje vprašanj o varnosti. Rezultati naše raziskave so pokazali, da se 36,54 % anketirancev nikoli ne prijavlja v elektronsko pošto iz javnih spletnih mest (npr. spletna kavarna, razne ustanove z uporabo brezplačne povezave). Letno – redko jo uporablja 34,62 %, nekajkrat na mesec - včasih 17,95 % v raziskavo zajetih medicinskih sester. V naši raziskavi smo o prepričanju kraje službenih podatkov iz službenega računalnika pridobili zanimive rezultate. Za možen scenarij kraje se je opredelilo 37,26 % medicinskih sester. Pri kraji z osebnega računalnika pa se je za možen scenarij opredelilo 46,40 % anketiranih. Pri mobilni telefoniji v krajo podatkov kot možen dogodek verjame 45,75 % anketiranih. V krajo identitete na svetovnem spletu (e-banka, Facebook, elektronska pošta) 25,49 % anketirancev ni prepričanih v celoti, kot mogoče se je opredelilo 35,95 % anketirancev.

Z zgoraj opisanim lahko ovržemo drugo hipotezo (H2), ki pravi: »Stopnja ozaveščenosti omenjene populacije o varnosti informacij je manjša kot 64,37 % «, saj rezultati jasno kažejo, da so anketiranci ozaveščeni o načinih varovanja informacij na družabnih omrežjih. Prav tako jih večina ne odpira neznane elektronske pošte. Elektronsko pošto neznanih pošiljateljev odpira brez preverjanje prilog 19,23 % medicinskih sester. Svojih osebnih podatkov (npr. osebni naslov, št. telefona, razna obvestila) na družabnih omrežjih ne objavlja 82,16 % anketiranih medicinskih sester. Zelo pomemben element zaščite je ločevanje poslovnih računalniških virov od osebnih (prenosni disk, elektronska pošta, telefon). Večina anketirancev (66,67 %) je omenjeno trditev ovrednotila kot zelo pomembno. Kot zelo pomembno je 69,39 % anketirancev označila preverbo tujega medija (USB ključek) pred uporabo, ali je okužen z virusi. Varovati pred krajo svoj USB disk oz. USB ključek s pomembnimi podatki, je kot zelo pomembno označilo kar 82,31 % anketirancev. Skladno s tem lahko ovržemo tretjo hipotezo (H3), ki pravi: »Uporabniška raven prepričanja o informacijski varnosti omenjene populacije je nižja kot 45 %«. Anketiranci menijo, da je shranjevanje dokumentov na dodatno lokacijo pomembo, prav tako tudi kopija podatkov. Rezultati pilotne študije Šolića in Ilakovčeve (2009) so bili s tega vidika slabi, saj je bila izdelava

varnostnih kopij v obeh skupinah (raziskovalci in pedagoški delavci uporabniki prenosnih računalnikov) zelo nizka. Omenjena študija je pokazala, da ima zavest uporabnikov o varnostnih tveganjih pomembno vlogo pri zagotavljanju zasebnosti podatkov. Večina anketirancev (65,99 %) meni, da je shranjevanje dokumentov še na dodatno lokacijo ali spominsko enoto (izdelava varnostne kopije podatkov) zelo pomembno; 26,03 % se jih ne spomni, kdaj so zadnjič naredili kopijo; 23,29 % je kopijo podatkov naredilo v zadnjih 6 mesecih; 8,90 % kopije ni naredilo nikoli.Večina je preverjanje USB-ja navedla kot zelo pomembno. Izdelava varnostne kopije podatkov lahko prepreči katastrofo (Bergen, 2005). Informacijski pooblaščenec pri uporabi prenosnih medijev priporoča sledenje uveljavljenim standardom v IS. Uporaba določenih izhodnih priključkov in naprav se dovoljuje le tistim zaposlenim, ki jih zaradi narave svojega dela potrebujejo (Informacijski pooblaščenec v sodelovanju s skupino za bolnišnične informacijske sisteme pri združenju zdravstvenih zavodov Slovenije, str. 10). Skladno z rezultati naše raziskave smo ovrgli četrto hipotezo (H4), ki se glasi: »Več kot 80 % omenjene populacije ima slabe navade pri zagotavljanju sistematičnih zamenjav vstopnih gesel.« Brezpogojno varovanje gesel je velika večina anketirancev (82,99 %) označila kot zelo pomembno. Kot zelo pomembno so označili tudi periodično zamenjavo gesel za pomembnejše sisteme, in sicer 61,91 % anketirancev. Glede na izračune, nižje izobražene medicinske sestre redkeje opravijo periodično zamenjavo gesel, medtem ko višje izobražene počnejo to pogosteje. Mlajše pogosteje opravijo periodično zamenjavo gesel za pomembnejše sisteme kakor starejše. Največ medicinskih sester, tj. 45,89 %, navaja, da poznajo geslo za dostop do elektronske pošte le one; v 45,21 % pa poleg njih pozna geslo še ena oseba. 8,22 % deli geslo s šedvema osebama. Medicinske sestre smo povprašali o posojanju plačilne kartice in PIN kode. Le 11,73 % anketirancev redko posoja svoje plačilne kartice in PIN kodo prijateljem, sorodnikom in znancem, medtem ko jih 84,57 % tega nikoli ne počne. Pri plačevanju s kartico jih 98,14 % nikoli z glasno izgovorjavo ne razkriva PIN kode. Pri odtujitvi denarja s tekočega računa je 41,18 % medicinskih sester navedlo, da je ta scenarij mogoč, 27,45 % ni povsem prepričanih in 5,23 % je popolnoma prepričanih.

Rezultati študije Albaraka (2011) kažejo, da se kar 92 % medicinskih sester strinja, da je načelo preverjanje pristnosti gesla pomembno, vendar je njihovo vedenje popolnoma nasprotno. To jasno kaže dejstvo, da 81 % anketirancev iz omenjene študije nikoli ni spremenilo gesla za dostop v IS, 54 % ni spremenilo gesla niti po vstopu nepooblaščenih oseb, 33 % je svoja gesla razkrilo sodelavcem, 32 % je omogočilo drugim uporabo svojih gesel in 16 % se jih ne odjavi iz aplikacij po končanem delu (Albarrak, 2011). Gesla morajo biti redno zamenjana in se z drugimi uporabniki ne delijo oziroma posojajo, ker je tako njihova učinkovitost ogrožena (NRC, 2011).

Z magistrsko nalogo smo skušali odgovoriti na vprašanje: »Ali je znanje medicinskih sester s področja informacijske varnosti zadostno, da pri svojem delu zagotovijo celovitost in zaupnost pacientovih zdravstvenih podatkov?« Glede na pregled tuje literature in interpretacijo rezultatov so mnenja različna. V nadaljevanju smo opisali nekatera od njih. Villanueva in sod. (2011) so ugotovili, da je za 63,7 % medicinskih sester v Španiji glavna ovira uporabe IKT pomanjkanje časa. Pomanjkanje usposabljanja je problem za 29,4 % medicinskih sester in le 7,5 % ni navedlo nobenih težav. Rezultati omenjene študije jasno kažejo, da se medicinske sestre soočajo z vrsto ovir pri vključevanju IKT v njihovo rutinsko delo (Villanueva in sod., 2011).

Kar je še najbolj sporno, je posojanje uporabniških imen in gesel. Po delu se v službi iz informacijskega sistema odjavi vedno 82,05 % anketirancev. Svoj računalnik zaklene, ko na kratko odide iz pisarne, od delovne mize na stranišče ali odmor le 36,54 % anketirancev, nikoli pa 21,79 %. IS, še posebej zdravstvene, lahko primerjamo z rudniki zlata zaupnih informacij. Medtem ko so uporabniki IKT nepazljivi, se lahko zgodi marsikaj. Podobno velja tudi pri problematiki izposojanja uporabniških imen in gesel, pa tudi odlaganje zdravstvenih kartonov na delovnih pultih (NRC, 2011). Iz opisanega lahko zaključimo, da se veliko medicinskih sester ne zaveda dovolj svoje odgovornosti. Določba (ZVOP), ki opredeljuje sledljivost obdelave OP, je izjemnega pomena predvsem za odkrivanje nepooblaščenih vstopov v zbirke OP in posledično zlorabe (npr. javno razkritje) (Informacijski pooblaščenec v sodelovanju s skupino za bolnišnične informacijske sisteme pri združenju zdravstvenih zavodov Slovenije, str. 6).

Za zmanjšanje kršitev informacijske varnosti v bolnišničnem okolju je treba povečati stopnjo ozaveščenosti pri medicinskih sestrah. Te morajo razumeti kritično naravo pacientovih podatkov, ki v nobenem primeru ne smejo biti dostopni nepooblaščenim osebam. Zavedati se je potrebno, da je informacijska varnost odgovornost vsakega zaposlenega posameznika. Potrebno je uveljavljanje varnostnih politik in spodbujanje zaposlenih za uskladitev z njimi (Albarrak, 2011).

Ne glede na število sodelujočih v raziskavi in način, na katerega je bil dostop do spletne ankete mogoč (objava na spletni strani društva, e-pošta in družabne strani), je vzorec kljub temu relevanten, saj ni bil fokusiran le na določeno organizacijsko enoto, temveč je zajel 174 strokovnjakov zdravstvene nege na slovenskem območju. Sama zavrnitev s strani Zbornice-Zveze in določenih strokovnih društev, prav tako posameznih organizacij, kaže predvsem na nezavedanje pomembnosti informacijske varnosti in morebiten strah pred rezultati, ki bi kazali na neznanje in nezavedanje medicinskih sester na področju varnosti IKT.

6 ZAKLJUČEK

Ne glede na pridobljene rezultate menimo, da je znanja s področja informacijske varnosti še vedno premalo. Predvsem je veliko medicinskih sester, pri katerih zaznavamo nezavedanje pomembnosti varovanja podatkov – ne glede na starost in delovne izkušnje. Kljub temu, da so bili deleži anketirancev z različnim ravnanjem na področju informacijske varnosti nizki, je lahko ravno ta skupina veliko tveganje za varnost zdravstvenega IS. Puščanje zdravstvenih kartonov in izvidov na delovnih mizah, hodnikih, bolniških mizicah, vozovih za jemanje krvi in vozovih za preveze, nepravilno uničenje in metanje dokumentov v smeti, dajanje informacij po telefonu, razlaga zdravstvenega stanja na hodniku in v sobi pred drugimi pacienti, pošiljanje predaje službe preko e-pošte, navsezadnje zapisana uporabniška imena in gesla ter njihovo posojanje sodelavcem, so le nekatere kršitve zasebnosti, za katere smo tudi zakonsko odgovorni in se v praksi dogajajo vsakodnevno.

Zdravstvena nega kot stroka nikakor ne sme spregledati ali celo ignorirati razvoja IKT in z njeno uporabo povezanimi varnostnimi vprašanji. Medicinske sestre ne smejo čakati, da bo IKT odgovorila na vprašanja, s katerimi se soočajo na delovnem mestu. Ne smejo imeti le pasivnega odnosa do omenjenih tehnologij, postati morajo napredni uporabniki IKT.

Informacijska varnost je nenehen izziv in varnostne kršitve, ki izhajajo iz uporabniškega nedostojnega vedenja, veljajo kot tveganje za kršitev zaupnosti pacientovih podatkov. Informacijska varnost, zasebnost in zaupnost pacientovih podatkov v okolju zdravstvene nege ne bi smeli biti obravnavani le kot politika in postopki, temveč kot kultura in praksa. V bodoče je potrebno medicinske sestre usposobiti za delo z IKT, predvsem pa z varnostjo. V izobraževalnem sistemu je treba nujno zagotoviti tako teoretične kakor praktične vsebine s področja informacijske varnosti, za zaposlene v zdravstvu in zdravstveni negi pa so nujna vsakoletna izobraževanja iz omenjene tematike ter morebitne sankcije ob ugotovitvi odklonov. Samo tehnični varnostni ukrepi ne morejo preprečiti kršitev informacijske varnosti in ravno ozaveščanje, usposabljanje in izobraževanje uporabnikov na omenjenem področju je pomembno za doseganje zanesljive ravni varnosti informacij v zdravstvenih organizacijah.

7 VIRI

ABBOTT, A. P. in COENEN, A., 2008. Globalization and advances in information and communication technologies. *Nursing outlook*, letn. 56, št. 5, str. 238-248.

AACN, 2011. New AACN data show growth in doctoral nursing programs [spletni vir]. [Datum dostopa 29. 5. 2015].
Dostopno na: http://www.aacn.nche.edu/news/articles/2010/enrollchanges

ALBARRAK, A., 2012. Information Security Behavior among Nurses in an Academic Hospital. HealthMED, letn. 6, št. 7, str. 2349-2354.

ALEMAN, F., in sod., 2014. Exploring the Use of information and communication technologies and social networks among university nursing faculty staff. An opinion survey. *Investigación y educación en enfermería*, letn. 32, št. 3, str. 438-450.

BAKKEN, S., 2006. Informatics for patient safety: A nursing research perspective. *Annual review of Nursing research,* letn. 24, št. 1, str. 219–254.

BARNARD, A. G., NASH, R. E., in O'BRIEN, M., 2005. Information literacy: developing life long skills through nursing education. *Journal of nursing education*, letn. 44, št. 11, str. 505-510

BERNARD, R., 2007. Information Lifecycle Security Risk Assessment: A tool for closing security gaps. *Computers & security*, letn. 26, št. 1, str. 26-30.

BARTON, A. J., 2005. Cultivating informatics competencies in a community of practice. *Nursing administration quarterly* , letn. 29, št. 4, str. 323-328.

BRATUŠA, T., 2007. *Hitri vodnik po zaščiti vašega računalnika – kako se izogniti neželeni pošti, virusom, vdorom in drugim nevšečnostim.* Ljubljana: Pasadena, str. 16, 117.

BRATUŠA, T., 2010. Več varovanja, manj varnosti? V: RODIČ B., ur. *Projektna organizacija dela in informacijska tehnologija in varnost informacijskih sistemov: zbornik prispevkov 3. posveta Dolenjskih in Belokranjskih informatikov*. Fakulteta za informacijske študije Novo mesto, str. 5-11.

BREZAVŠČEK, A. in MOŠKON, S., 2010. Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji [spletni vir]. *Uporabna informatika*, letn. 18, št. 2, str. 101-108. [Datum dostopa 29. 5. 2015]
Dostopno na
http://www.vris.si/Db/vris/content/pdf/Brezascek_Moskon_InfoKomTeh_2009_prispevek.PDF.

BREZOVŠEK, M., in ČRNEC, D., 2007. *Demokratična uprava in tajnost podatkov*. Ljubljana: Fakulteta za družbene vede, str. 115, 116, 195, 196.

BERNIK, I. in PRISLAN, K., 2012. Information security in risk management systems: Slovenian perspective [spletni vir]. *Varstvoslovje*, letn. 13, št. 2, str. 208-222. [Datum dostopa 29. 5. 2015]
Dostopno na http://www.fvv.um.si/varstvoslovje/articles/vs-2011-2-07_bernik-prislan.pdf

BERGEN, D. M., 2005. Data integrity: backup. *The journal of school nursing*, letn. 21, št. 1, str. 60-62.

CHANG, J., POYNTON, R. M., GASSERT, A. C. in STAGGERS, N., 2011. Nursing informatics competencies required of nurses in Taiwan. *International journal of medical informatics*, letn. 80, št. 5, str. 332–340.

CUNNINGHAM, B. in sod., 2007. The best damn IT security management book period [spletni vir]. Burlington, ZDA: Syngress Publishing, Inc., str. 688-715. [Datum dostopa 29. 5. 2015] Dostopno na http://www.sciencedirect.com/science/book/9781597492270

ČELEBIĆ, G. in RENDULIĆ, D. I., 2012. ITdesk.info – načrtovanje računalniškega e-izobraževanja s prostim dostopom - priročnik za digitalne pismenosti [spletni vir]. Otvoreno društvo za razmjenu ideja (ODRAZI), Zagreb, str. 1, 28-29. [Datum dostopa 28. 5. 2015]. Dostopno na http://www.itdesk.info/slo/prirocnik/prirocnik_osnovni_pojmi_informacijske_tehnologije.pdf

DAMRONGSAK, M. in BROWN, K. C., 2008. Data security in occupational health. *American Association of Occupational Health Nurses;* letn. 56, št. 10, str. 417-421.

DESJARDINS, K. S., COOK, S., JENKINS, M. in BAKKEN, S., 2005. Effect of an informatics for Evidence-based Practice Curriculum on nursing informatics competencies. *International journal of medical informatics*, letn. 74, št. 11-12, str. 1012-1020.

DELOITTE, 2011. Raising the bar: 2011 TMT global security study e keyfindings [spletni vir]. [Datum dostopa 20. 5. 2015]. Dostopno na: http://d20tdhwx2i89n1.cloudfront.net/image/upload/t_attachment/geqo8ae6wi7q7fdwzopp.pdf.

DIMITROPOULOS, L. in RIZK, S., 2009. A state-based approach to privacy and security for interoperable health information exchange. *Health affairs*, str. 428-434.

DIXON, B. E. in NEWLON, M. C., 2010. How Do Future Nursing Educators Perceive Informatics? Advancing the Nursing Informatics Agenda through Dialogue, *Journal of professional nursing*, letn. 26, št. 2, str. 82 – 89.

DOWDING, D., 2013. Are nurses expected to have information technology skills? *Nursing management*; letn. 20, št. 5, str. 31-37.

EGAN, M. in MATHER T., 2005. *Varovanje informacij: grožnje, izzivi in rešitve: vodnik za podjetja*. Kraj: Založba Pasadena, str. 16, 33, 107.

ELOFF, J. H. P in ELOFF, M., 2005. Integrated Information Security Architecture. *Computer fraud and security*, letn. 11, št. 10, str. 6.

ERNST, YOUNG, 2011. Into the cloud, out of the fog: Global information security survey [spletni vir]. [Datum dostopa: 17. 12. 2015].

Dostopno na: http://www.shinnihon.or.jp/shinnihon library/publications/research/2012/pdf/2011-GlobalInformationSecuritysurvey-E.pdf

FURNELL, S., JUSOH, A., KATSABAS, D., 2006. The challenges of understanding and using security: A survey of end-users. *Computers & security*, letn. 25, št. 1, str. 27-35.

FETTER, M. S., 2009a. Improving information technology competencies: implications for psychiatric mental health nursing. *Issues in mental health nursing*, letn. 30, št. 1, str. 3-13.

FETTER, M. S., 2009b. Baccalaureate Nursing Students' Information Technology Competence—Agency Perspectives. *Journal of professional nursing*, letn. 25, št. 1, str. 42-49.

FORBES, A. in WHILE, A., 2009. The nursing contribution of chronic disease management: a discussion paper. *International journal of nursing studies*, letn. 46, št. 1, str. 120–131.

GLASER, J. in ASKE, J., 2010. Healthcare IT trends raise bar for information security. *Healthcare financial management*, letn. 64, št. 7, str. 40-44.

GRIFFITH, R., 2007. Understanding confidentiality and disclosure of patient information. *British journal of community nursing*, letn. 12, št. 11, str. 530-534.

HAISA, 2007. *Proceedings of the International Symposium on Human Aspects of Information Security and Assurance*. V: FURNELL S., CLARKE N., ur. Information Security & Network Research Group, University of Plymouth.

HART, M., 2008. Informatics competency and development within the US nursing population workforce. *Computers, informatics, nursing*, letn. 26, št. 6, str. 320-329.

IOM, 2010. The future of nursing: Focus on education [spletni vir]. *National Academy of Sciences*, str. 1-7. [Datum dostopa 20. 5. 2015]. Dostopno na http://www.iom.edu/~/media/Files/Report%20Files/2010/The-Future-of-Nursing/Nursing%20Education%202010%20Brief.pdf

Informacijski pooblaščenec v sodelovanju s skupino za bolnišnične informacijske sisteme pri združenju zdravstvenih zavodov Slovenije, 2008. Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic [spletni vir]. [Datum dostopa 30. 7. 2015]. Dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_zavarovanje_OP_v_IS_bolnisnic_15022008.pdf

KUMMETH, P., LAUREL B., CAIRNE, E. in FRAZIN, K., 2007. An Ethical View: Security at Your Fingertips. *Minnesota nursing accent*, str. 8-9.

KOVAČIČ, M., 2006. *Nadzor in zasebnost v informacijski družbi; filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu*. Univerza v Ljubljani: Fakulteta za družbene vede, str. 7, 8, 11, 12, 44.

OVIJAČ, D., VELEPIČ, M., ADAMIČ, M., EDER, BUČEK HAJDAREVIĆ, I., KARDOŠ, Z., KLEMENC, D., et al. 2014. *Kodeks etike v zdravstveni negi in*

oskrbi Slovenije. Ljubljana: Zbornica zdravstvene in babiške nege Slovenije - Zveza strokovnih društev medicinskih sester in zdravstvenih tehnikov Slovenije.

KRUGER H. A. in KEARNEY, W. D., 2006. A prototype for assessing information security awareness. *Computers and security*, letn. 25, št. 4, str. 289–96.

LANDOLL, D. J., 2006. *The security risk assessment handbook: A complete guide for performing security risk assessments* [spletni vir]. New York: Taylor & Francis Group, LLC, str. 15, 154, 229. [Datum dostopa 10. 5. 2015]
Dostopno na http://www.leetupload.com/database/Misc/Papers/Auerbach.Publications,.The.Security.Risk.Assessment.Handbook.%282005%29.DDU.LotB.pdf

LILLY, K., FITZPATRICK, J. in MADIGAN, E., 2015. Barriers to Integrating Information Technology Content in Doctor of Nursing Practice Curricula. *Journal of professional nursing*, letn. 31, št. 3, str. 187-199.

LINEBERRY, S., 2007. The human element: The weakest link in information security. *Journal of accountancy*, letn. 204, št. 5, str. 44-49.

MARCKMANN, G. in GOODMAN, K., 2006. Introduction: Ethics of Information Technology in Health Care [spletni vir]. *International review of information ethics*, letn. 5, št. 0, str. 2-5. [Datum dostopa 10. 5. 2015]
Dostopno na http://www.i-r-i-e.net/inhalt/005/Marckmann-Goodman.pdf

Mc NEIL, B. J., ELFRINK, V. L., PIERCE, S. T., BEYA, S. C., BICKFORD, C. J. in AVERILL, C., 2005. Nursing informatics knowledge and competencies: A national survey of nursing education programs in the United States. *International journal of medical informatics*, letn. 74, št. 11-12, str. 1021-1030.

MYLONAS, A., KASTANIA, A. in GRITZALIS, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computer & security*, letn. 34, št. 0, str. 47-66.

NG, B. Y., KANKANHALLI, A. in XU, Y., 2009. Studying users' computer security behavior: a health belief perspective [spletni vir]. *Decision support system*, letn. 46, št. 4, str. 815-825. [Datum dostopa 10. 5. 2015]
Dostopno na http://www.pacis-net.org/file/2007/1217.pdf

NRC, 2011. Can you handle all of you information? *Nursing & residental care*, letn. 13, št. 3, str. 144-146.

NIEKERK, J. F. in SOLMS, R., 2010. Information security culture: A management perspective. *Computers & security*, letn. 29, št. 4, str. 476-486.

O'CONOR, T., 2014. Maintaining safety and privacy in a digital world. *Nursing New Zealand*, letn. 20, št. 10, str. 23.

PARSONS, K., CORMAC, M. A., BUTAVICIUS, M., PATTISON in M., JERRAM, 2014. Determining employee awareness using the Human Aspects of Information Security Questionnarie (HAIS-Q). *Computer & security*, letn. 42, str. 165-176.

PAHNILA, S., SIPONEN, M. in MAHMOOD, A., 2007. Employees' Behavior towards IS Security Policy Compliance [spletni vir]. V: SPRAGUE R.H., ur. *System Sciences, 40th Annual Hawaii International Conference on System Sciences*. Big Island, Hawai: Los Vaqueros Circle, str. 156-156. [Datum dostopa 10. 5. 2015]

Dostopno na http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.7038&rep=rep1&type=pdf

PATTINSON, M. R. in ANDERSON, G., 2007. How well are information risks being communicated to your computer end-users? *Information management & computer security*, letn. 15, št. 5, str. 362-371.

PINCUS, J. D., 2005. Computer science is really a social science [spletni vir]. *Microsoft Research* [Datum dostopa 10. 5. 2015]
Dostopno na http://www.achangeiscoming.net/docs/cssocsci.html

RÅHOLM, M. B., THORKILDSEN, K. in LÖFMARK, A., 2010. Translation of the Nursing Clinical Facilitators Questionnaire (NCFQ) to Norwegian language. *Nurse education in practice*, letn. 10, št. 4, str. 196–200.

HERATH, T., RAO, H. R., 2009. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decisions support systems*, letn. 47, št. 2, str. 154–165.

SHEWCHUK, R., O'CONNOR, S. in FINE, D., 2005. Building an understanding of the competencies needed for health administration practice. *Journal of healthcare management*, letn. 50, št. 1, str. 32–47.

SHULTZ, C. M., 2009. Preparing to work in an informatics-based world [spletni vir]. *Imprint*, str. 36. [Datum dostopa 7. 11. 2015].
Dostopno na http://www.nsna.org/Portals/0/Skins/NSNA/pdf/Imprint_AprMay09_Feat_Shultz.pdf.

STANTON, J. M., STAM, K. R., MASTRANGELO, P. in JOLTON, J., 2005. Analysis of end user security behaviors. *Computer & security*, letn. 24, št. 2, str. 166-176.

SSKJ - Slovar slovenskega knjižnega jezika, 2000. Inštitut za slovenski jezik Frana Ramovša ZRC SAZU - Portal BOS [spletni vir]. Slovenska akademija znanosti in umetnosti. [Datum dostopa 7. 11. 2015].
Dostopno na http://bos.zrc-sazu.si/sskj.html.

SKIBA, D. J. in RIZZOLO, M. A., 2009. National League for Nursing's Informatics Agenda [spletni vir]. *Computers Informatics Nursing*, letn. 27, št.1, str. 66-68. [Datum dostopa 7. 11. 2015].
Dostopno na http://journals.lww.com/cinjournal/Citation/2009/01000/National_League_for_Nursing_s_Informatics_Agenda.14.aspx.

SVETE, U. in PINTERIČ, U., 2008. *E-država: upravno-varnostni vidiki.* Nova Gorica: Fakulteta za uporabne družbene študije, str. 72, 76.

ŠOLIĆ, K., VELIKI, T. in GALBA, T., 2015. Empirical study on ICT system's users' risky behavior and security awareness. V: BILJANOVIĆ, P., ur. *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*. IEEE. Rijeka: MIPRO str. 1356-1359.

ŠOLIĆ, K., VELIKI, T. in OČEVČIĆ, H., 2014. Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work". V: BILJANOVIĆ,

P., BUTKOVIĆ, Z., SKALA, K, ur. *Information and Communication Technology, Electronics and Microelectronics (MIPRO),37th International Convention on IEEE*. Opatija: IEEE, str. 1564-1568.

ŠOLIĆ, K., JOVIĆ, F. in BLAŽEVIĆ, D., 2013. An approach to the assessment of potentially risky behavior of ict systems' users [spletni vir]. *Tehnicki vjesnik-Technical Gazette*, letn. 20, št. 2, str. 335-342. [Datum dostopa 7. 11. 2015] Dostopno na http://hrcak.srce.hr/file/147724

ŠOLIĆ, K., GRGIĆ, K. in GALIĆ, D., 2010. A Comparative Study of the Security Level among Different Kind of E-mail Services – Pilot Study [spletni vir]. *Tehnicki vjesnik-Technical gazette,* letn. 17, št. 4, str. 489-492. [Datum dostopa 7. 11. 2015]
Dostopno na http: //hrcak.srce.hr/file/94281

ŠOLIĆ, K. in ILAKOVAC, V., 2009. Security Perception of a Portable PC User (The Difference Between Medical Doctors and Engineers): A Pilot Study. *Medicinski glasnik*; letn. 6, št. 2, str. 261-264.

TIGER, 2009. *Informatics Competencies Collaborative Final Report – August 2009* [spletni vir]. TIGER Initiative: str. 10. [Datum dostopa: 7. 11. 2015]. Dostopno na http://tigercompetencies.pbworks.com/f/TICC_Final.pdf.

TRČEK, D., TROBEC, R., PAVEŠIĆ, N. in TASIČ, J. F., 2007. Information system security and human behavior. *Behavior & information technology*, letn. 26, št. 1, str. 113-118.

VERDONIK, I. in BRATUŠA, T., 2005. *Hekerski vdori in zaščita*. Ljubljana: Pasadena, str. 96, 97, 222-224.

VEIGA, D. A. in ELOFF, J. H. P., 2010. A framework and assessment instrument for information security culture. *Computers & security*, letn. 29, št. 2, str. 196-207.

VILLANUEVA, F. L., HARDEYC, M., TORRENTD, J. in FICAPALD, P., 2011. The integration of Information and Communication Technology into nursing. *International journal of medical informatics*, letn. 80, št. 2, str. 133-140.

WEBER, E. J., GUSTER, D., SAFONOV P. in SCHMIDT, M. B., 2008. Weak password security: An empirical study. *Information security journal: a global perspective*, letn. 17, št. 1, str. 45-54.

WESTRA, B. L. in DELANEY, C. W., 2008. Informatics competencies for nursing and healthcare leaders. V: SUERMONDT, J., OHNO-MACHADO, L., EVANS, S., ur. *AMIA Annual Symposium Proceedings*. Kraj: American Medical Informatics Association, str. 804-808.

WHILE, A. in DEWSBURY, G., 2011. Nursing and information and communication technology (ICT): a discussion of trends and future directions. *International journal of nursing studies*, letn. 48, št. 10, str. 1302- 1310.

WIN, K. T., 2005. A review of security of electronic health records. *Health information management*, letn. 34, št. 1, str. 13-18.

NIIMI, Y. in OTA, K., 2014. Privacy Recognition by Nurses and Necessity of Their Information Security Education. V: SHAW, T. ur. *International Conference on*

Education Reform and Modern Management [spletni vir].Amsterdam: Atlantis Press, str. 358-361. [Datum dostopa: 7. 11. 2015].
Dostopno na www.atlantis-press.com/php/download_paper.php?id=11304.

Zakon o varstvu osebnih podatkov, 2007. Uradni list Republike Slovenije, št. 94/2007, 14. in 24. člen.

POVZETEK

Teoretična izhodišča: Največja nevarnost razkritja osebnih podatkov za področje zdravstvene nege je zaposleni v zdravstvenem varstvu, ki se ne zaveda in ne ve, kako pomembna je sama zaupnost podatkov. Številne študije poročajo o neustreznem vedenju medicinskih sester, zato je njegovo poznavanje še kako pomembno.

Metode dela: Raziskava med slovenskimi medicinskimi sestrami je potekala od 29. 4. 2015 do 31. 8. 2015 s pomočjo spletne ankete, v kateri je sodelovalo 174 anketirancev iz primarnega, sekundarnega in terciarnega zdravstvenega varstva ter socialno - varstvenih zavodov.

Rezultati: Raziskava je pokazala, da medicinske sestre v 64,81 % nikoli ne posojajo gesla za dostop do računalnika. Elektronsko pošto neznanih pošiljateljev nikoli ne odpira brez preverjanja prilog 73,08 % vprašanih. Po delu se iz informacijskega sistema vedno odjavi 82,05 %, po zapustitvi delovne postaje slednjo zaklene le 36,54 % anketirancev.

Razprava: V zdravstveni negi rezultati prikazane študije kažejo, da približno dve tretjini medicinskih sester upošteva varnostne ukrepe, vendar jih tretjina ukrepov ne upošteva. Sprašujemo se, kaj to pomeni na področju varovanja svojih osebnih podatkov in kaj je preneseno na področje varovanja osebnih podatkov pacienta, do katerih imajo dostop medicinske sestre, ki ne skrbijo za informacijsko varnost.

Zaključek: Problematika nerazumevanja informacijske varnosti predstavlja tempirano bombo na področju varovanja osebnih pacientovih podatkov. V povezavi s pridobljenimi rezultati lahko razmišljamo o tem, da se nevarnost uhajanja podatkov diagonalno veča z večanjem uporabe IT. Glede na trende uvajanja e-zdravja v slovenski prostor lahko trdimo, da je nujno potrebno dodatno opolnomočiti medicinske sestre z znanjem in poudariti pomen informacijske varnosti.

Ključne besede: zdravstvena nega, informacijska varnost, varnostno vedenje, varovanje podatkov.

SUMMARY

Theoretical assumptions: The greatest danger of personal data disclosure in the field of health care is the employee in health care, who is not aware and does not know the importance of the confidentiality of the data itself. Numerous studies have reported improper behaviour of the nursing staff, therefore the knowledge regarding this matter is ever so important.

Methods: An online survey was held among Slovenian nurses from 29.4.2015 to 31.8.2015, in which 174 subjects responded. The subjects were from the primary, secondary and tertiary health care and social care institutions.

Results: The study showed that 64.81% of nurses never lend their password to access the computer. 73.08% of the respondents state that they never open e-mails from unknown senders without checking the attachment. When finished working 82.05% of the respondents always checkes out of the information system, but only 36.54% of the respondents locks the computer after leaving the workstation.

Discussion: In the health care department the results of the presented study show that about two-thirds of the nurses comply with the security measures, whereas a third of them does not take the appropriate/applied measures. We wonder what this means firstly for the protection of their personal information and later on how this affects the protection of personal data of the patient, to which the nurses that do not take care of security have access to.

Conclusion: The problematic of misunderstanding of the information security represents a time bomb in the field of protection of personal patient data. In conjunction with the results obtained we can think about the fact that the risk of data leakage increases in congruence with the increased use of IT. Considering the trends of implementing the system E-health in the Slovenian space, we can safely say that it is necessary to further empower nurses with the knowledge and emphasize the significance of information security.

Key words: health care, information security, security behaviour, data protection.

ZAHVALA

Do dobrega življenja vodita ljubezen in znanje.
Ljubezen ga navdihuje, znanje usmerja.
Bertrand Russell

Za sodelovanje, pomoč in dosegljivost pri pisanju magistrske naloge gre posebna zahvala mentorju doc. dr. Boštjanu Žvanut in somentorici mag. Tamari Štemberger Kolnik, ki sta me tekom pisanja dela spodbujala in mi delila strokovne nasvete s svojega področja. Prav tako se zahvaljujem Ani Šegrt, uni. dipl. slavistki in primerjalni jezikoslovki za lektoriranje naloge.

Posebna zahvala gre mami in očetu, saj sta mi stala ob strani v času študija, me spodbujala, z mano delila vse dobre in slabe trenutke in me vedno nasmejala ter vlivala pogum.

Hvala vam za vso pomoč in dejanja, ki so moj študij privedla h koncu.

PRILOGA 1

Agreement for using and translating the Users' Information Security Awareness Questionnaire (UISAQ) in Slovenian language

To: Samanta Mikuletič and Boštjan Žvanut, University of Primorska, Faculty of health sciences

I agree to abide by the following principles in using the UISAQ questionnaire as a research tool:
- The questionnaire should only be used in its original form and translated in Slovene language (minor alternations are permissible, for example in order to ensure that the terminology reflects different cultural aspects). All other changes should be reported to the authors.
- Any research reports that have used the UISAQ questionnaire should acknowledge the original source by using the following reference: T. Velki, K. Solic and H. Ocevcic, "Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work", Proceedings IEEE MIPRO, (Opatia), pp. 1417-1421, May 2014.

Osijek, 20. 2. 2015

Krešimir Šolić

PRILOGA 2

VPRAŠALNIK ZA PREPOZNAVANJE VEDENJA IN OCENO ZNANJA INFORMACIJSKE VARNOSTI

Spoštovani. Sem Samanta Mikuletič, študentka 2. letnika podiplomskega magistrskega programa 2. stopnje (zdravstvena nega), FVZ Izola. V okviru zaključne naloge raziskujem in pišem o informacijski varnosti na področju zdravstvene nege. Sodelovanje v anketi je ključnega pomena in osnova, na kateri lahko oblikujem in gradim zaključno nalogo, zato Vas prosim za pomoč. Pred Vami je anketa, s katero bi rada ugotovila, kakšne so navade medicinskih sester pri uporabi informacijsko-komunikacijskih računalniških sistemov. Študije o tej temi so zelo redke, za stroko zdravstvene nege pa izjemno pomembne, saj zadevajo celovitost pacientovih podatkov, njihovo zaupnost, poklicno etiko in pravne zadeve. Prosim, da si vzamete nekaj minut in iskreno ter v popolnosti odgovorite na vprašanja. Sodelovanje je anonimno.

Hvala. Samanta Mikuletič

Spol:

◌ Moški
◌ Ženski

Starost - navedite starost _____

Kakšna je Vaša najvišja dosežena formalna izobrazba?

◌ Srednješolska (zdravstveni tehnik/srednja medicinska sestra)
◌ Višješolska (višja medicinska sestra)
◌ Visokošolska 1. stopnje (diplomirana medicinska sestra/zdravstvenik)
◌ Visokošolska 2. stopnje (magister zdravstvene nege)
◌ Visokošolska 3. stopnje (doktorat znanosti)
◌ Drugo: _____

Vaše delovno mesto sodi v raven/zavod:

◌ Primarno zdravstveno raven
◌ Sekundarno zdravstveno raven
◌ Terciarno zdravstveno raven
◌ Socialno - varstveni zavod

Ali doma (osebni računalnik) uporabljate avtentifikacijske podatke/dostopno geslo za računalnik? Ali se je za dostop do računalnika treba prijaviti z geslom?

◌ da
◌ ne

Ali v službi (službeni računalnik) uporabljate avtentifikacijske podatke/dostopno geslo za računalnik? Ali se je za dostop do računalnika treba prijaviti z geslom?

- ◌ da
- ◌ ne

V preglednicah so navedene trditve, ki predstavljajo običajna vedenja uporabnikov računalniške komunikacijske tehnologije. Prosimo Vas, da pozorno preberete opis posamezne trditve in ustrezno označite odgovor, ki nakazuje Vaše ravnanje v povezavi z dano trditvijo.

	Nikoli	Redko (letno)	Včasih (mesečno)	Pogosto (tedensko)	Vedno (dnevno)
Avtentifikacijske podatke (uporabniško ime in geslo) posojam sodelavcem v službi, ko jih potrebujejo.	◌	◌	◌	◌	◌
Avtentifikacijske podatke (uporabniško ime in geslo) za osebni (domač) računalnik, posojam svojim prijateljem, sorodnikom, znancem.	◌	◌	◌	◌	◌
Avtentifikacijske podatke (uporabniško ime in geslo) za prijavo v osebno elektronsko pošto posojam prijateljem, sorodnikom, znancem.	◌	◌	◌	◌	◌
Svoje plačilne kartice in PIN-kodo posojam svojim prijateljem, sorodnikom, znancem.	◌	◌	◌	◌	◌
Z glasno izgovarjavo razkrivam svojo PIN kodo prodajalcu, ko plačujem s plačilno kartico v trgovini.	◌	◌	◌	◌	◌
Za različne informacijske komunikacijske sisteme (Facebook, elektronska pošta, poslovni računi) uporabljam različna vstopna gesla.	◌	◌	◌	◌	◌
Vzdržujem zaščito svojega osebnega računalnika z rednimi posodobitvami, antispaywari in antivirusnimi programi.	◌	◌	◌	◌	◌
Redno vzdržujem nadgradnjo vseh uporabniških programov in operacijskega sistema na osebnem računalniku.	◌	◌	◌	◌	◌
Na svoj osebni računalnik nameščam razne programe neznanih/manj znanih avtorjev, ki so zanimivi, niso pa nujno potrebni (video player, multimedijski dodatki).	◌	◌	◌	◌	◌
Osebne podatke objavljam na družabnih omrežjih (npr. osebni naslov, številko telefona, obvestilo da sem na dopustu).	◌	◌	◌	◌	◌
Odpiram in odgovarjam na elektronsko pošto neznanih pošiljateljev.	◌	◌	◌	◌	◌
E-pošto neznanih pošiljateljev odprembrez preverjanja prilog.	◌	◌	◌	◌	◌
Pošiljam/posredujem verižno e-pošto.	◌	◌	◌	◌	◌
Uporabljam več elektronskih naslovov (npr. osebno in službeno).	◌	◌	◌	◌	◌
V e-pošto se prijavljam z različnih javnih spletnih mest (npr. spletna kavarna, razne ustanove, z uporabo brezplačne povezave).	◌	◌	◌	◌	◌

E-pošto neznanih pošiljateljev odprembrez preverjanja prilog.	○	○	○	○	○
Po končanem delu se iz informacijskega sistema odjavim.	○	○	○	○	○
Svoj računalnik zaklenem, ko na kratko odidem iz pisarne, od delovne mize na stranišče ali odmor.	○	○	○	○	○

Prosimo Vas, da pozorno preberete trditve ter v pripadajoči stolpec označite, koliko je trditev po vašem mnenju varna.

	Popolnoma nevarno	Razmeroma nevarno	Ne vem	Razmeroma varno	Popolnoma varno
Dopisovanje preko e-pošte.	○	○	○	○	○
Komunikacija preko družabnih omrežji (npr. Facebook).	○	○	○	○	○
Komunikacija preko mobilnega telefona (pogovor, sporočila).	○	○	○	○	○
Komunikacija preko stacionarnega telefona.	○	○	○	○	○
Komunikacija preko svetovnega spleta (npr. Skype, Viber, Chat).	○	○	○	○	○

Prosimo Vas, da pozorno preberete navedene trditve ter v pripadajoči stolpec ustrezno označite stopnjo prepričanja, da se Vam bo navedena trditev zgodila/uresničila.

	Nisem prepričan v celoti	Mogoče	Ne vem	Deloma prepričan	Popolnoma prepričan
Da Vam bo nekdo ukradel službene podatke s službenega računalnika (v organizaciji, kjer delate).	○	○	○	○	○
Da Vam bo nekdo ukradel podatke z osebnega računalnika.	○	○	○	○	○
Da Vam bo nekdo ukradel podatke z mobilnega telefona.	○	○	○	○	○
Da Vam bo nekdo odtujil denar s tekočega računa.	○	○	○	○	○
Da Vam bo nekdo ukradel identiteto na svetovnem spletu (e-banka, Facebook, e-pošta).	○	○	○	○	○

Prosimo Vas, da pozorno preberete navedene trditve ter ocenite, koliko je pomembno izvajati zapisane aktivnosti. Pomembnost označite v stolpcu, ki to izraža.

	Popolnoma nepomembno	Deloma nepomembno	Ne vem	Deloma pomembno	Zelo pomembno
Shraniti pomembne dokumente še na dodatno lokacijo/spominsko enoto (varnostna kopija podatkov).	○	○	○	○	○
Pred uporabo (pred pregledovanjem podatkov) tujega USB medija preveriti ali je okužen z virusi.	○	○	○	○	○
Brezpogojno varovanje svojih gesel.	○	○	○	○	○
Periodična zamenjava gesel za pomembnejše sistem.	○	○	○	○	○
Ločiti poslovne računalniške vire od osebnih (prenosni disk, elektronska pošta, telefon).	○	○	○	○	○
Varovati pred krajo svoj USB disk (USB ključ) s pomembnimi podatki.	○	○	○	○	○

	Nikoli	Ne spomnim se	V 6 mesecih	V mesecu dni	Prejšnji teden
Kdaj ste zadnjič naredili varnostno kopijo osebnih podatkov/dokumentov?	○	○	○	○	○

	Več kot 10	Več kot 5	Jaz in še 2 osebi	Jaz in še 1 oseba	Samo jaz
Koliko oseb pozna geslo za pristop v Vašo elektronsko pošto?	○	○	○	○	○

PRILOGA 3

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Ispitivanje ponašanja i znanja korisnika o pitanjima koja se tiču informacijske sigurnosti.	Anketa za ugotavljanje vedenja in znanja uporabnikov o vprašanjih, ki se nanašajo na informacijsko varnost.	Vprašalnik o obnašanju uporabnikov o informacijski varnosti.	Vprašalnik za prepoznavanje vedenja in uporabe znanja v informacijski varnosti.	Vprašalnik za prepoznavanje vedenja in oceno znanja o informacijski varnosti.	Vprašalnik za prepoznavanje vedenja in oceno znanja informacijske varnosti (MS/študentov ZN).	Upitnik za identifikaciju ponašanja i procjenu znanja vezanih uz informacijsku sigurnost.
Ova anketa je namijenjena svim osobama koja se koriste računalima. Cilj je saznati navike korisnika različitih informacijsko-komunikacijskih računalnih sustava. Anketa je u potpunosti anonimna stoga vas molim da iskreno odgovorite na sva pitanja.	Anketa je namenjena uporabnikom računalnika. Cilj je ugotoviti navade uporabnikov različnih informacijsko-komunikacijskih sistemov. Anketa je anonimna, zato Vas prosim, da iskreno odgovorite na vsa vprašanja.	Anketa je namenjena vsem osebam, ki uporabljajo osebne računalike. Cilj je ugotoviti navade uporabnikov različnih informacijsko-kounikacijskih računalniških sistemov. Anketa je popolnoma anonimna, zato vas prosimo, da odgovorite na vsa vprašanja.	Vprašalnik je namenjen vsem uporabnikom osebnih računalikov. Cilj je ugotoviti navade uporabnikov različnih informacisjko komunikacijskih računalniških sistemov. Anketa je popolnoma anonimna, zato vas prosimo, da odgovorite na vsa vprašanja.	Vprašalnik je namenjen vsem uporabnikom osebnih računalikov. Cilj je ugotoviti navade uporabnikov različnih informacisjko kounikacijskih računalniških sistemov. Anketa je popolnoma anonimna, zato vas prosimo, da odgovorite na vsa vprašanja.	Vprašalnik je namenjen uporabnikom (medicinskim sestram/študentom zdravstene nege) osebnih računalikov. Cilj je ugotoviti navade uporabnikov različnih informacisjko kounikacijskih računalniških sistemov. Sodelovanje je popolnoma anonimno, zato vas prosimo, da odgovorite na vsa vprašanja.	Upitnik je namijenjen svim korisnicima osobnih računala. Cilj je identificirati navike korisnika različitih informacijsko komunikacijskih sustava. Upitnik je u potpunosti anoniman, stoga vas molimo da odgovorite na sva pitanja.
Spol (muško/žensk)	Spol (moški/ženski)	Spol	Spol (moški/ženski)	Spol	Spol (moški/ženski)	Spol
Koliko imate godina?	Starost _____	Vnesite št. dopolnjenih let	Starost - označite	Starost (lestvica)	Starost - označite	Dob (ljestvica)
Koja ste stručna sprema: a) nkv b) sss c) sšs (gimnazija) d) všs e) vssmr.sc., dr.sc. Ili više	Stopnja izobrazbe a) osnovna šola b) srednja strokovna sola c) gimnazija d) višja šola e) visoka šola f) magister znanosti/doktor znanosti	Dosežena stopnja izobrazbe: a) osnovna šola ali manj b) poklicna šola c) gimnazija d) višješolska izobrazba e) magister znanosti f) doktor znanosti	Zaključena stopnja izobrazbe: a)srednja strokovna izobrazba b)gimnazija c)višja ali visoka d)univerzitetna ali več	Dosežena izobrazba: a)srednješolska (zdravstveni tehnik), b)višješolska (višja MS) c)visokošolska 1. stopnje (DMS/zdravstvenik), d)visokošolska 2. stopnje (mag. ZN), e)visokošolska 3. stopnje (doktorat znanosti) f) drugo:_____	Dosežena izobrazba: a)srednješolska (zdravstveni tehnik), b)višješolska (višja MS) c)visokošolska 1. stopnje (DMS/zdravstvenik), d)visokošolska 2. stopnje (mag. ZN), e)visokošolska 3. stopnje (doktorat znanosti) f) drugo:_____	Dosežena izobrazba: a)srednješolska (zdravstveni tehnik), b)višješolska (višja MS) c)visokošolska 1. stopnje (DMS/zdravstvenik), d)visokošolska 2. stopnje (mag. ZN), e)visokošolska 3. stopnje (doktorat znanosti) f) drugo:_____

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Vaše radno mjesto: a)uprava-viši management b)voditelji odjela i slično-niži management c)zaposlenik	Vaše delovno mesto: a)uprava (višji/vršni management) b)vodja oddelka srednji management c) delavec (nižji management)	Vaše delovno mesto: a)uprava (všji management) b)vodja oddelka in podobno (nižji management) c) zaposlenec brez vodstvenih funkcij	Vaše delovno mesto: a)vršni managment b)srednji managment (vodja oddelka ali enote) c)operativni managment (zaposleni brez vodstvene funkcije)	Vaše delovno mesto: a)vršni managment b)srednji managment (vodja oddelka ali enote) c)operativni managment (zaposleni brez vodstvene funkcije)	Vaše delovno mesto sodi v raven/zavod: a)Primarno zdr. raven b)Sekundarno zdr. raven c)Terciarno zdr. raven d)Socialno-varstveni zavod	
Radi analize i procjene kvalitete zaporke molimo vas čitko napišite vašu trenutnu zaporku za pristup sustavu elektroničke pošte (anketa je anonimna):	Za namene analize in oceno kakovosti prosim, da jasno napišite svoje trenutno geslo za dostop do elektronske pošte (anketa je anonimna):	Za namen analize in oceno kakovosti prosimo, da jasno napišite trenutno dostopno geslo do elektronske pošte (sodelovanje je anonimno):	Za namen analize in oceno kakovosti prosimo, da jasno napišite trenutno dostopno geslo do elektronske pošte (sodelovanje je anonimno):	Za namen analize in oceno kakovosti prosimo, da jasno napišite trenutno dostopno geslo do elektronske pošte (sodelovanje je anonimno):	Za namen analize in oceno kakovosti prosimo, da jasno napišite trenutno dostopno geslo do elektronske pošte (sodelovanje je anonimno):	U svrhu analize i procjene kvalitete, molimo da jasno napišete trenutnu zaporku za pristup vašoj elektronskoj pošti (anketa je anonimna)
U slijedećoj tablici opisane su neke situacije koje opisuju uobičajena ponašanja korisnika računalnih informacijsko-komunikacijskih sustava. Molimo vas da pažljivo pročitate opis pojedinih ponašanja i situacija te da u odgovarajući stupac ispod učestalosti s „x“ označite koliko ste se često ponašali na određeni način.	V naslednji tabeli so opisane situacije, katere opisujejo pogosta vedenja uporabnikov računalniških informacijsko komunikacijskih sistemov. Prosimo vas da pozorno preberete opis posameznih vedenj in situacij/položaj, ter, da v želeni stolpec pogostost s »x« označite kako pogosto ste počeli naštete stvari na določen način.	V naslednji preglednici so predstavljene nekatere, ki opisujejo ustaljena obnašanja uporabnikov računalniških informacijsko-komunikacijskih sistemov. Prosimo vas, da pozorno prečitate opis posameznih obnašanj in situacij ter v pripadajoči stolpcu ustrezno označite pogostost (v vsaki vrstici po en odgovor).	V naslednji preglednici so predstavljene trditve, ki predstavljajo običajne vedenjske situacije uporabnikov računalniške komunikacijske tehnologije. Prosimo vas, d apozorno preberete opis posameznih vedenj in situacij. V stolpcu ustrezno označite z »x« odgovor, ki nakazuje na vaše ravnanje v povezavi z dano trditvijo.	V naslednji preglednici so predstavljene trditve, ki predstavljajo običajne vedenjske situacije uporabnikov računalniške komunikacijske tehnologije. Prosimo vas, da pozorno preberete opis posamezne situacije v stolpcu ustrezno označite z »x« odgovor, ki nakazuje na vaše ravnanje v povezavi z dano trditvijo.	V preglednici so navedene trditve, ki predstavljajo običajne vedenjske situacije uporabnikov računalniške komunikacijske tehnologije. Prosimo vas, da pozorno preberete opis posamezne trditve in ustrezno označite odgovor, ki nakazuje vaše ravnanje v povzavi z dano trditvijo.	U sljedećoj tablici su opisane tvrdnje koje predstavljaju uobičajene situacije i ponašanja korisnika računalno-komunikacijske tehnologije. Molimo vas da pažljivo pročitate pojedine situacije te u stupcu pravilno označite sa "x" odgovor koji označava vaše postupanje u vezi sa zadanom tvrdnjom
Situacije koliko često činite sljedeće?	Situacije/položaj kako pogosto počnete naslednje?	Situacije-koliko pogosto počnete naslednje?	Situacija kako pogosti vi to počnete?	Situacij - kako pogosto počnete naslednje?	Kako pogosto počnete naslednje:	Situacija-koliko često radite sljedeće?
Učestalost	Pogostost	Pogostost	Pogostost	Pogostost	Pogostost	Učestalost
Nikad	Nikoli	Nikoli	Nikoli	Nikoli	Nikoli	Nikada
Rijetko nekoliko godišnje	Redko (nekajkratna leto)	Redko (nekajkrat na leto)	Redko (nekajkratna leto)	Redko (nekajkrat na leto)	Redko (nekajkrat na leto)	Rijetko (nekoliko godišnje)
Ponekad (nekoliko puta mjesečno)	Včasih (nekajkrat na mesec)	Včasih (nekajkrat na mesec)	Včasih (nekajkrat na mesec)	Včasih (nekajkrat na mesec)	Včasih (nekajkrat na mesec)	Ponekad (nekoliko puta mjesečno)

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Često (nekoliko puta tjedno)	Pogosto (nakajkrat na teden)	Pogosto (nakajkrat na teden)	Pogosto (nakajkrat na teden)	Pogosto (nekajkrat na teden)	Pogosto (nekajkrat na teden)	Često (nekoliko puta tjedno)
Uvijek (skoro svaki dan)	Vedno (skoraj vsak dan)	Vedno (skoraj vsak dan)	Vedno (skoraj vsak dan)	Vedno (skoraj vsak dan)	Vedno (skoraj vsak dan)	Uvijek (skoro svaki dan)
Posuđujete službene pristupne podatke (korisničko ime i zaporka) kolegama studentima ili na poslu, koji se nađu u potrebi (npr. Za vrijeme bolovanja, godišnjeg).	Posojate službene dostopne podatke (uporabniško ime in geslo), sodelavcem, študentom, zaposlenemu, ki nadomešča odsotnega (čas bolniške, letnega dopusta).	Posojate službene avtentifikacijske podatke (uporabniško ime in geslo) sodelavcem v službi, ki jih potrebujejo (npr. Za čas bolniške, dopusta).	Avtentifikacijske podatke (uporabniško ime in geslo) posojam sodelavcem v službi, ko jih potrebujejo (čas bolniške odsotnosti, dopust).	Avtentifikacijske podatke (uporabniško ime in geslo) posojam sodelavcem v službi, ko jih potrebujejo (čas bolniške odsotnosti, dopust).	Avtentifikacijske podatke (uporabniško ime in geslo) posojam sodelavcem v službi, ko jih potrebujejo (čas bolniške odsotnosti, dopust).	Podatke za autentifikaciju (korisničko ime i zaporku/lozinku) posuđujem suradnicima na poslu kada im je potrebno (za vrijeme bolovanja, godišnjeg dmora).
Posuđujete svojim prijateljima, rođacima, poznanicima svoje privatne pristupne podatke za pristup kućnome računalu.	Posojate svojim prijatelje, sorodnikom, znancem svoje privatne dostopne podatke za dostop do osebnega računalnika.	Posojate svojim prijateljiem, sorodnikom, znancem svoje privatne avtentfikacijske podatke za prijavo v domači osebni računalnik.	Avtentifikacijske podatke (uporabniško ime in geslo) za osebni (domač) računalnik, posojam svojim prijateljem, sorodnikom, znancem.	Avtentifikacijske podatke (uporabniško ime in geslo) za osebni (domač) računalnik, posojam svojim prijateljem, sorodnikom, znancem.	Avtentifikacijske podatke (uporabniško ime in geslo) za osebni (domač) računalnik, posojam svojim prijateljem, sorodnikom, znancem.	Posuđujem podatke za autentifikaciju (korisničko ime i zaporku) za osobno (kućno) računalo svojim prijateljima, rođacima, poznanicima.
Posuđujete svojim prijateljima, rođacima, poznanicima svoje privatne pristupne podatke za pristup osobnoj/privatnoj e-mail adresi.	Posojate prijateljem, sorodnikom, znancem svoje pristopne podatke za dostop do osebne/privatne e-mail naslova.	Posojate svojim prijateljiem, sorodnikom, znancem svoje privatne avtentfikacijske podatke za prijavo v osebni/privatni e-mail.	Avtentifikacijske podatke (uporabniško ime in geslo) za prijavo v osebno elektronsko pošto posojam prijateljem, sorodnikom, znancem.	Avtentifikacijske podatke (uporabniško ime in geslo) za prijavo v osebno elektronsko pošto posojam prijateljem, sorodnikom, znancem.	Avtentifikacijske podatke (uporabniško ime in geslo) za prijavo v osebno elektronsko pošto posojam prijateljem, sorodnikom, znancem.	Podatke za autentifikaciju (korisničko ime i zaporku) za prijavu na osobnu elektronsku poštu posuđujem svojim prijateljima, rođacima, poznanicima.
Posuđujete svojim prijateljima, rođacima, poznanicima svoje privatne kreditne kartice i pripadajući pin.	Posojate prijateljem, sojcem in znancem svoje kreditne kartice in pripadajoči pin.	Posojate svojim prijateljiem, sorodnikom, znancem svoje privatne kreditne kartice in pripadajoči pin.	Svoje kreditne kartice in pin-kodo posojam svojim prijateljem, sorodnikom, znancem.	Svoje kreditne kartice in pin-kodo posojam svojim prijateljem, sorodnikom, znancem.	Svoje kreditne kartice in pin-kodo posojam svojim prijateljem, sorodnikom, znancem.	Svoje kreditne kartice i pin broj posuđujem prijateljima, rođacima i poznanicima
Otkrivate svoj pin (neskrivanjem, glasnim izgovaranjem prodavaču) kada plaćate karticom u trgovini.	Razkrivate svoj pin (neskrivanjem, glasno izgvorjavo trgovcu) ko plačate s kartico v trgovini.	Razkrivate svoj pin (neskrivanjem, glasnim izgovarjanjem prodajalcu), ko plačujete s kreditno kartico v trgovini.	Z glasnim izgovarjanjem razkrivam svojo pin kodo prodajalcu, ko plačujem s kreditno kartico v trgovini.	Z glasnim izgovarjanjem razkrivam svojo pin kodo prodajalcu, ko plačujem s kreditno kartico v trgovini.	Z glasno izgovorjavo razkrivam svojo pin kodo prodajalcu, ko plačujem s kreditno kartico v trgovini.	Kada plaćam s kreditnom karticom u trgovini glasnim izgovaranjem otkrivam svoj pin broj prodavaču

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Koristite različite zaporke za različite sustave, npr. Za facebook jedna, za mail druga, za poslovni sustav treća lozinkaitn.	Uporabljate različna gesla za različne sisteme, npr. Za facebook eno, za mail drugega, za poslovni sistem tretjega, itd.	Uporabljate različna gesla za različne sisteme (npr. Facebook, drugo za email, tretje za poslovni račun itn.).	Za različne informacijske komunikacijske sisteme (Facebook, elektronaka pošta, poslovni računi) Uporabljam različna vstopna gesla.	Za različne informacijske komunikacijske sisteme (Facebook, elektronaka pošta, poslovni računi) Uporabljam različna vstopna gesla.	Za različne informacijske komunikacijske sisteme (Facebook, elektronska pošta, poslovni računi) uporabljam različna vstopna gesla.	Za različite informacijsko-komunikacijske sustave (Facebook, elektronička pošta, poslovni računi) koristim različite pristupne zaporke
Održavate zaštitu svoga privatnog računala odnosno radite li nadogradnju (engl. update) antispayware i antivirusnih programa	Vzdržujete zaščito svojega osebnega računalnika oziroma, naredite posodobitve (eng. Update) antispayware in antivirusnihprogramov.	Vzdržujete zaščito svojega provatnega osebnega računalnika in redno izvajate posodobitev (angl. "update") antispayware in antivirusnih programov	Vzdržujem zaščito svojega osebnega računanika z rednimi posodobitvami (ang. Update), antispayware in antivirusnih programov	Vzdržujem zaščito svojega osebnega računanika z rednimi posodobitvami (ang. Update), antispayware in antivirusnih programov	Vzdržujem zaščito svojega osebnega računanika z rednimi posodobitvami (ang. Update), antispayware in antivirusnih programov.	Održavam zaštitu svog osobnog računala s redovnim nadogradnjama/ažuriranjem (eng. Update), antispayware i antivirusnim programima
Vršite nadogradnju i ostalih korisničkih programa te operativnog sustava na vašem privatnom računalu	Upravljate posodobitve uporabniških programov in operativnega sistema na vašem privatnem računalniku.	Izvajate nadgradnjo tudi ostalih uporabniških programov in operacijskega sistema na vašem privatnem računalniku	Redno vzdržujem nadgradnjo vseh uporabniških programov in operacijskega sistema na osebnem računalniku.	Redno vzdržujem nadgradnjo vseh uporabniških programov in operacijskega sistema na osebnem računalniku.	Redno vzdržujem nadgradnjo vseh uporabniških programov in operacijskega sistema na osebnem računalniku.	Redovno održavam nadogradnju svih korisničkih programa i operacijskog sustava na osobnom računalu
Instalirate razne programe nepoznatih i manje poznatih proizvođača koji su možda zanimljivi no nisu stvarno neophodni (npr. razni video playeri, multimedijalni dodaci web preglednicima).	Inštalirate/namestite razne programe nepoznanih in manj poznanih proizvajalce ki so zanimivi, niso pa ravno potrebni (npr. razni vido player, multimedijski dodatki web preglednic).	Nameščate razne programe neznanih in manj poznanih proizvajalcev, ki so morda zanimivi in niso dejansko nujno potrebni (npr. razni video playeri, multimedijski dodatki preglednicima).	Na svoj osebni računalnik namestite razne programe neznanih ali mnaj poznanih avtorjev, ki so vam zanimivi niso pa nujno potrebni (video player).	Na svoj osebni računalnik nameščam razne programe neznanih ali manj poznanih avtorjev, ki so mi zanimivi niso pa nujno potrebni (recimo: video player, multimedijski dodatki).	Na svoj osebni računalnik nameščam razne programe neznanih ali manj poznanih avtorjev, ki so zanimivi, niso pa nujno potrebni (recimo: video player, multimedijski dodatki).	Na svoje osobno računalo instaliram razne programe nepoznatih ili manje poznatih autora, koji su mi zanimljivi, no nisu nužno i potrebni (recimo: video-player, multimedijski dodaci).
Ostavljate osobne podatke na društvenim mrežama (npr. Privatnu adresu, broj mobitela, poruku da ste na godišnjem i sl.).	Puščate osebne podatke na družbenih omrežjih (naslov bilvališča, številko mobitela, sporočilo da ste na počitnicah in podobno).	Ostavljate osebne podatke na socialnih omrežjih (npr. Zasebni naslov, številko mobitela, obvestilo (post), da ste na letnem dopustu ipd.).	Osebne podatke zabeležite (objavite) na socialnih omrežjih (npr. osebni naslov, številko telefona, obvestilo d aste na dopustu).	Osebne podatke zabeležujem (objavljam na socialnih omrežjih (npr. osebni naslov, številko telefona, obvestilo da ste na dopustu).	Osebne podatke zabeležujem/objavljam na socialnih omrežjih (npr. osebni naslov, številko telefona, obvestilo da sem na dopustu).	Osobne podatke (npr. kućnu adresu, broj telefona, obavijest da ste na godišnjem odmoru) ostavljam zabilježene (objavljujem ih na socijalnim mrežama).
Odgovarate na mailove od nepoznatih/sumnjivih pošiljatelja.	Odgovarjate na elektronsko pšto nepoznanih/sumljivih pošiljateljev.	Odgovarjate na e-maile neznanih oz. Sumljivih pošiljateljev.	Odgovarjam na elektronsko pošto neznanih sumljivih pošiljateljev.	Odgovarjam na elektronsko pošto neznanih sumljivih pošiljateljev.	Odgovarjam na elektronsko pošto neznanih/sumljivih pošiljateljev.	Odgovaram na elektronsku poštu nepoznatih, sumnjivih pošiljatelja.

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Otvarate, bez provjere, priloge od nepoznatih pošiljatelja.	Odpirate priloge od nepoznanih pošiljateljev brez prevarjanja.	Odpirate brez da bi preverili priloge neznanih pošiljateljev.	Elektronsko pošto neznanih pošiljateljev odprem brez, da bi preveril priloge.	Elektronsko pošto neznanih pošiljateljev odprem brez, da bi preveril priloge.	Elektronsko pošto neznanih pošiljateljev odprem brez preverjanja prilog.	Elektronsku poštu nepoznatih pošiljatelja otvaram bez provjeravanja privitka.
Prosljeđujete/šaljete lančane mailove (npr. poruke o donacijama, sreći i sl.).	Posredujete/pošiljate verižna sporočila (npr. sporočila o donacijah, sreči itd.).	Posredjete (angl. forward) oz. pošiljate verižne emaile mailove (npr. Sporočila o donacijah ipd.).	Pošiljam/posredujem erižne elektronske pošte (sporočila o donacijah).	Pošiljam/posredujem (angl. "forward") verižno elektronsko pošto (sporočila o donacijah).	Pošiljam/posredujem (angl. "forward") verižno elektronsko pošto (sporočila o donacijah).	Šaljem ili proslijeđujem lančanu elektronsku poštu (npr. poruke za donacije i sl.).
Koristite više e-mail adresa (npr. privatni i službeni e-mail).	Uporablajte več e-mail naslovov (npr. osebnega in službenega).	Uporabljate več e-mail naslovov (npr. Privatni in službeni e-mail).	Uporabljamm več el. naslovov (npr. osebno in službeno pošto).	Uporabljam več elektronskih naslovov (osebno in službeno).	Uporabljam več elektronskih naslovov (osebno in službeno).	Koristim više adresa el. adresa/e-mail adresa (privatnu i službenu).
Prijavljujete se na vaš e-mail s različitih javnih mjesta (internet kafići, razne ustanove, korištenjem besplatne wifi mreže).	Prijavljate se na vaš e-mail z različnih javnih mest (internetne kavarne, razne ustanve), s uporabo wi-fi mreže itd.	Prijavljate se v vaš poštni predal z različitih javnih mesta (skavarne, razne ustanove), z uporabo brezplačne wi-fi omrežja. ipd.).	Na poštni predal elektronske pošte se prijavljam z različnih javnih spletnih mest (npr. spletna kavarna, razne ustanove), z uporabo wi-fi povezave.	Na poštni predal elektronske pošte se prijavljam z različnih javnih spletnih mest (spletna kavarna), z uporabo wi-fi povezave.	V elektronsko pošto se prijavljam z različnih javnih spletnih mest (npr. spletna kavarna, razne ustanove), z uporabo brezžične wi-fi povezave.	Na poštanski pretinac elektronske pošte se prijavljujem s različitih mrežnih stranica (npr. internet kafić), korištenjem bežične wi-fi veze.
Odjavljujete se sa informacijskog sustava prilikom završetka rada.	Po končanem delu se odjavite iz informacijskega sistema.	Odjavljate se iz informacijskega sistem ob zaključenem delu.	Po končanem delu na spletnem mediju se redno odklapljam.	Po končanem delu se z informacijskega sistema odjavim.	Po končanem delu se iz informacijskega sistema odjavim.	Nakon završenog rada, odjavim se s informacijskog sustava.
Zaključavate službeno računalo prilikom kraćeg odlaska iz ureda, učionice, radnog stola na primjer na toalet ili pauzu.	Zaklenete službeni računalnik ko odidete na kratki iz pisarne, učilnice, delovnega sedeža na wc ali pavzo.	Zaklepate osebni računalnik ob krajšem izhodu iz pisarne, učilnice, delovne mize, ko greste npr. na wc ali pavzo.	Svoj računalnik zaklenem ko na kratko odidem iz pisarne, učilnice, delovne mize, na stranišče ali odmor.	Svoj računalnik zaklenem ko na kratko odidem iz pisarne, učilnice, delovne mize, na stranišče ali odmor.	Svoj računalnik zaklenem ko na kratko odidem iz pisarne, učilnice, delovne mize, na stranišče ali odmor.	Zaključavam svoje računalo ako na kratko izađem iz ureda, učionice, radnog stola na toalet ili na odmor.
Molimo vas da pažljivo pročitate opis pojedinih situacija te da u odgovarajući stupac ispod stupnja sigurnosti označite koliko su prema vašem mišljenju situacije sigurne.	Prosim va da previdno preberete opis posamezne situacije in da v odgovarjajoči stolpec pod stopnjo varnosti označite kolikokrat so po vašem mižljenje sledeče situacije varne.	Prosimo, vas da pozorno preberete opis posazenih situacij ter v pripadajočem stolpcu ustrezno označite, koliko so po vašem mnenjeu situacije varne (v vsaki vrstici en odgovor).	Prosimo vas, da pozorno preberete navedene trditve ter po vašem mnenju ocenite njihovo stopnjo varnosti in to označite v odovarjajočem stolpcu.	Prosimo vas da pozorno preberete navedene trditve, ter v pripadajočem stolpcu ustrezno označite, koliko so po vašem mnenju varne (v vsaki vrstici po en odgovor).	Prosimo vas, da pozorno preberete trditve, ter v pripadajoči stolpec označite, koliko je trditev po vašem mnenju varna (v vsaki vrstici po en odgovor).	Molimo vas da pažljivo pročitate navedene tvrdnje te u odgovarajućem stupcu pravilno označite koliko je po vašem mišljenju sigurno (u svakom redku jedan odgovor).
Što mislite koliko je sigurno:	Koliko je varno?	Kaj mislite, da je (ne)varno?	Kaj menite, koliko je varno?	Kaj menite, koliko je varno?	Kaj menite, koliko je varn?	Po vašem mišljenju koliko je sigurno?

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Potpuno nesigurno	Popolnoma nevrano	Popolnoma nevarno	Popolnoma nevarno	Popolnoma nevarno	Popolnoma nevarno	Potpuno nesigurno
Prilično nesigurno	Precej nevarno	Razneroma nevarno	Razneroma nevarno	Razmeroma nevarno	Razmeroma nevarno	Donekle nesigurno
Ne znam	Ne vem	Niti varno niti nevarno	Niti varno niti nevarno	Ne vem	Ne vem	Ne znam
Prilično sigurno	Precej varno	Razneroma varno	Razneroma varno	Razmeroma varno	Razmeroma varno	Donekle sigurno
Potpuno sigurno	Popolno varno	Popolnoma varno	Popolnoma varno	Popolonoma varno	Popolonoma varno	Potpuno sigurno
Dopisivanje putem e-pošte	Dopisovanje preko e-pošte	Dopisovanje preko e-pošte	Dopisovanje po e-pošti	Dopisovanje po e-pošto	Dopisovanje preko e-pošte	Dopisivanje putem e- pošte
Komunikacija putem društvenih mreža (npr. Facebook, twitter).	Komunikacija preko družbenih omrežij (npr, Facebook, twiter).	Komunikacija preko socialnih omrežij (npr. Facebook, twitter).	Komunikacija preko socialnih omrežji (np. Facebook).	Komunikacija preko socialnih omrežji (np. Facebook).	Komunikacija preko socialnih omrežji (np. Facebook.)	Komunikacija putem socijalnih mreža (npr. Facebook).
Komunikacija mobitelom (razgovori, sms)	Komunikacija preko mobitela (razgovori, sms)	Komunikacija preko mobilnega telefona (pogovori, sms)	Komunikacija preko mobilnega telefona (pogovor, sporočila)	Komunikacija preko mobilnega telefona (pogovor, sporočila)	Komunikacija preko mobilnega telefona (pogovor, sporočila	Komunikacija mobilnim telefonom (razgovori, poruke/sms)
Komunikacija žičnim telefonom	Komunikacija preko stac. telefona	Komunikacija z običajnim telefonom	Komunikacija preko stac. telefona	Komunikacija preko stac. telefona	Komunikacija preko stac telefona	Komunikacija fiksnim telefonom
Općenito komunikacija putem interneta (npr. Skype, viber, chat)	Na splošno komunikacija preko interneta (npr. Skype, viber, chat)	Komunikacija preko svetovnega spleta (npr. Skype, viber, chat).	Komunikacija preko svetovnega spleta (npr. Skype, viber, chat)	Komunikacija preko svetovnega spleta (npr. Skype, viber, chat)	Komunikacija preko svetovnega spleta (npr. Skype, viber, chat)	Komunikacija putem interneta (npr. Skype, viber, chat)
Molimo vas da pažljivo pročitate opis pojedinih situacija te da u odgovarajući stupac ispod stupnja uvjerenje označite koliko ste uvjereni da će vam se dogoditi sljedeće situacije.	Prosimo vas da previdno preberete opis posameznih situacij in da v odgovarjajoči stolpec pod stopnjo prepričanje označite koliko ste prepričani v sledeče situacije.	Prosimo vas, da pozorno preberete navedene trditve ter v pripadajočem stolpcu ustrezno označite stopnjo prepričanja, da se vam bodo navedene situacije zgodile.	Prosimo vas, da pozorno preberete opis posameznih dejanj in ocenite stopnjo možnosti uresničitve navedenih dejanj. Oceno označite v pripadajočem stolpcu.	Prosimo vas, da pozorno preberete navedene trditve ter v pripadajočem stolpcu ustrezno označite stopnjo prepričanja, da se vam bodo navedene situacije zgodile.	Prosimo vas, da pozorno preberete navedene trditve ter v pripadajoči stolpec označite stopnjo prepričanja, da se vam bo navedena trditev zgodila/uresniči la.	Molimo vas da pažljivo pročitate tvrdnje te u odgovarajućem stupcu označite stupanj uvjerenja da će vam se dogoditi navedene situacije.
Koliko ste uvjereni da postoji realna opasnost:	Koliko ste prepričani da obstoja realna nevarnost:	Koliko ste uvjereni da postoji realna opasnost:	Koliko ste prepričani v predsatvljeno nevarnost:	Koliko ste prepričani v predsatvljeno nevarnost:	Koliko ste prepričani v predsatvljeno nevarnost:	Koliko ste uvjereni u navedenu opasnost :
Stupanj uvjerenja	Stopnja prepričanja	Stopnja prepričanja	Stopnja prepričanja	Stopnja prepričanja	Stopnja prepričanja	Stupanj uvjerenja
Nisam uvjeren/a	Nisem prepričan	Nisem prepričan v celoti	Nisem prepričan v celoti	Nisem prepričan v celoti	Nisem prepričan v celoti	Nisam uvjeren/a u potpunosti
Možda	Mogoče	Nisem prepričan deloma	Mogoče	Mogoče	Mogoče	Možda
Ne znam	Ne vem	Niti prepričan niti nisem prepričen	Ne vem	Ne vem	Ne vem	Ne znam
Prilično	Dokaj	Prepričan - deloma	Prepričan - deloma	Deloma prepričan	Deloma prepričan	Djelomično sam uvjeren/a

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Potpuno	Popolnoma	Prepričan - popolnoma	Popolnoma preprčan	Popolnoma preprčan	Popolnoma preprčan	U potpunosti sam uvjeren/a
Da će vam netko ukrasti službene podatke sa službenog računala (u firmi ili na fakultetu).	Da vam bo nekdo ukradel službene podatke iz službenega računalnika (v podjetju ali na fakulteti).	Da vam bo nekdo ukradel službene podatke s službenega računalnika (v organizaciji, kjer delate).	Da vam bo nekdo ukradel službene podatke iz službenega računalnika (v službi).	Da vam bo nekdo ukradel službene podatke s službenega računalnika (v organizaciji, kjer delate).	Da vam bo nekdo ukradel službene podatke s službenega računalnika (v organizaciji, kjer delate).	Da će vam netko ukrasti službene podatke sa službenog računala (u organizaciji u kojoj radite).
Da će vam netko ukrasti privatne podatke s vašeg kućnog računala.	Da vam bo nekdo ukradel privatne/osebne podatke s vašega osebnega računalnika.	Da vam bo nekdo ukradel podatke z domačega osebnega računalnika.	Da vam bo nekdo ukradel podatke z osebnega računalnika.	Da vam bo nekdo ukradel podatke z osebnega računalnika.	Da vam bo nekdo ukradel podatke z osebnega računalnika	Da će vam netko ukrasti podatke s mobilnog telefona .
Da će vam netko ukrasti privatne podatke s vašeg mobilnog uređaja.	Da vam bo nekdo ukradel privatne/osebne podatke z vašega mobilnega telefona.	Da vam bo nekdo ukradel zasebne podatke z vaše mobilne naprave.	Da vam bo nekdo ukradel podatke z mobilnega telefona.	Da vam bo nekdo ukradel podatke z mobilnega telefona.	Da vam bo nekdo ukradel podatke z mobilnega telefona.	Da će vam netko ukrasti podatke s mobilnog telefona.
Da će vam netko otuđiti novac s vašeg računa u banci.	Da vam bo nekdo odujil denar z vašega bančnega računa.	Da vam bo nekdo vzel denar z vašega tekočega računa.	Da vam bo nekdo odtujil denar z vašega tekočega računa.	Da vam bo nekdo odtujil denar z vašega tekočega računa.	Da vam bo nekdo odtujil denar z vašega tekočega računa.	Da će vam netko otuđiti novac s vašeg tekućeg računa.
Da će vam netko ukrasti identitet na internetu (e-banking, face, mail).	Da vam bo nekdo ukradel identiteto na internetu (e-banka, facebook, mail).	Da vam bo nekdo ukradel vašo identiteto na iternetu (npr. E-bančništvo, facebook, mail).	Da vam bo nekdo ukradel vašo identiteto na svetovnem spletu (e-banka, facebook, e-pošta)	Da vam bo nekdo ukradel vašo identiteto na svetovnem spletu (e-banka, facebook, e-pošta)	Da vam bo nekdo ukradel vašo identiteto na svetovnem spletu (e-banka, facebook, e-pošta)	Da će vam netko ukrasti identitet na internetu (e-banka, facebook, elektronska pošta)
Molimo vas da pažljivo pročitate opis pojedinih situacija te da u odgovarajući stupac ispod stupnja važnosti označite koliko je prema vašem mišljenju važno raditi sljedeće stvari.	Prosim vas da pozorno preberete opis posameznih situacij in da v odgovarjajoči stolpec pod stopnjo varnsti označite koliko je po vašem mišljenju pomembno delati naštete stvari.	Prosimo vas, da pozorno preberete opis posameznih situacij ter da v pripadajoči stolpec odogovrite, koliko je po vašem mnenju pomebno delati naslednje stvari.	Prosimo vas, da pozorno preberete navedene tditve, po vašem nenju ocenite koliko je pomembno izvajati predstavljene aktivnosti in to označite v stolpcu, ki to izaža.	Prosimo vas, da pozorno preberete navedene tditve, ter ocenite koliko je pomembno izvajati zapisane aktivnosti in to označite v stolpcu, ki to izaža.	Prosimo vas, da pozorno preberete navedene tditve, ter ocenite koliko je pomembno izvajati zapisane aktivnosti. Pomembnost označite v stolpcu, ki to izaža.	Molimo vas da pažljivo pročitate navedene tvrdnje i procijenite koliko je važno izvoditi napisane aktivnosti te označite u odgovarajućem stupcu.
Prema vašem mišljenju koliko je važno	Po vašem mnenju, koliko je pomembno	Koliko je po vašem mnenju pomembno?	Po vašem mnenju koliko je to pomembno	Koliko je po vašem mnenju pomembno?	Koliko je po vašem mnenju pomembno?	Koliko je po vašem mišljenju važno?
Stupanj važnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stupanj važnosti

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Potpuno nevažno	Popolnoma nepomembno	Popolnoma nepomembno	Popolnoma nepomembno	Popolnoma nepomembno	Popolnoma nepomembno	Potpuno nevažno
Prilično nevažno	Povsem nepomembno	Deloma nepomembno	Deloma nepomembno	Deloma nepomembno	Deloma nepomembno	Djelomično nevažno
Ne znam	Ne vem	Niti pomembno niti nepomombno	Ne vem	Ne vem	Ne vem	Ne znam
Prilično važno	Deloma pomembn	Deloma pomembno	Deloma pomembno	Deloma pomembno	Deloma pomembno	Djelomično važno
Izrazito važno	Zelo pomembno	Zelo (popolnoma) pomembno	Zelo pomembno	Zelo pomembno	Zelo pomembno	Izrazito važno
Kopirati važnije dokumente na još jednu, drugu lokaciju odnosno drugi memorijski uređaj (izrada pričuvnih kopija podataka).	Kopirati pomembne dokumente na še eno drugo lokacijo oziroma drugi spominsko opremo (izdelava rezervnih kopij podatkov).	Kopirati pomembne dokumente še na eno drugo lokacijo oziroma na drugo spominsko enoto (izdelava varnostnih kopij podatkov).	Shranjevati pomembne dokumente še na eni lokaciji ali spominski enoti (oblikovanje kopij pomenbnih podatkov).	Shraniti pomembne dokumente še na eno lokacijo ali spominsko enoto (izdelava varnostnih kopij podatkov).	Shraniti pomembne dokumente še na dodatno lokacijo ali spominsko enoto (izdelava varnostnih kopij podatkov).	Pohraniti važne dokumente na još jednu lokaciju ili memorisjku jedinicu (izrada sigurnosnih kopija podataka).
Provjeriti tuđi usb memorijski štapić od virusa prije učitavanja podataka.	Preveriti tuji usb ključek zaradi virusov pred nalaganjem podatko.	Preveriti je tuj usb disk (usb ključ) okužen z virusi pred pregledovanjem podatkov.	Pred uporabo tujih usb medijev za prenos podatkovnih baz, preveriti ali so okuženi z virusi.	Pred uporabo tujega usb medija preveriti ali jr okužen z virusi, pred pregledovanjem podatkov.	Pred uporabo (pred pregledovanjem podatkov) tujega usb medija preveriti ali je okužen z virusi.	Prije učitavanja podataka s tuđeg usb medija, provjeriti je li zaražen virusom.
Bezuvjetno čuvati tajnost svojih zaporki.	Brezpogojno varovati tajnost svojih gesel	Brezpogojno varovati tajnost svojih gesel.	Brezpogojno varovanje svojih gesel.	Brezpogojno varovanje svojih gesel.	Brezpogojno varovanje svojih gesel.	Bezuvjetno zaštiti svoje zaporke.
Periodično zamijeniti svoje zaporke novima, barem za važnije sustave.	Periodično zamenjati svoja gesla z novimi, vsaj za pomembnejše sisteme.	Periodično zamenjati svoja gesla, vsaj za pomembnejše sisteme.	Za pomembneješe sisteme pogosto menjavanje vstopna gesla.	Periodično zamenjati gesla za pomembneješe sisteme.	Periodična zamenjava gesel za pomembneješe sistem.	Povremeno mijenjati zaporke za najvažnije sustave.
Odvajati poslovne računalne resurse od privatnih (npr. prijenosna memorija, elektronička pošta, telefon).	Ločiti poslovne računalniške vire od osebnih (prenosni disk, elektroska pošta, telefon).	Ločiti poslovne računalniške resurse od zasebnih (npr. Prenosni disk, elektronska pošta, telefon).	Ločiti poslovne vire od osebnih (npr. Prenosni disk, elektronska pošta, telefon).	Ločiti poslovne računalniške vire od osebnih (prenosni disk, elektroska pošta, telefon).	Ločiti poslovne računalniške vire od osebnih (prenosni disk, elektroska pošta, telefon).	Odvojiti poslovne računalne resurse od osobnih (prijenosni diks, elektronska pošta, telefon).
Čuvati od krađe svoj usb memorijski štapić sa važnim podacima.	Varovati pred krajo svoj usb ključek s pomembnimi podatki.	Varovati od kraje svoje usb disk (usb ključ) s pomembnimi podatki.	Pred krajo dobro zaščititi usb medij s pomembnimi podatki.	Varovati od kraje svoje usb disk (usb ključ) s pomembnimi podatki.	Varovati od kraje svoje usb disk (usb ključ) s pomembnimi podatki.	Čuvati od krađe svoj usb s važnim podacima.
Molimo vas da pažljivo pročitate opis pojedinih situacija te da u odgovarajući stupac ispod stupnja uvjerenje označite koliko	Prosimo vas da previdno preberete opis posameznih situacij in da v odgovarjajoči stolpec pod stopnjo prepričanje označite koliko	Prosimo vas, da pozorno preberete navedene trditve ter v pripadajočem stolpcu ustrezno označite stopnjo	Prosimo vas, da pozorno preberete opis posameznih dejanj in ocenite stopnjo možnosti uresničitve navedenih dejanj. Oceno	Prosimo vas, da pozorno preberete navedene trditve ter v pripadajočem stolpcu ustrezno označite stopnjo	Prosimo vas, da pozorno preberete navedene trditve ter v pripadajoči stolpec ustrezno označite stopnjo	Molimo vas da pažljivo pročitate tvrdnje te u odgovarajućem stupcu označite stupanj uvjerenja da će vam se dogoditi navedene

ste uvjereni da će vam se dogoditi sljedeće situacije.	ste prepričani v sledeče situacije.	prepričanja, da se vam bodo navedene situacije zgodile.	označite v pripadajočem stolpcu	prepričanja, da se vam bodo navedene situacije zgodile.	prepričanja, da se vam bo navedena trditev zgodila/uresničila.	situacije
Koliko ste uvjereni da postoji realna opasnost:	Koliko ste prepričani da obstoja realna nevarnost:	Koliko ste uvjereni da postoji realna opasnost:	Koliko ste prepričani v predsatvljeno nevarnost:	Koliko ste prepričani v predsatvljeno nevarnost:	Koliko ste prepričani v predsatvljeno nevarnost:	Koliko ste uvjereni u navedenu opasnost:
Stupanj uvjerenja	Stopnja prepričanja	Stopnja prepričanja	Stopnja prepričanja	Stopnja prepričanja	Stopnja prepričanja	Stupanj uvjerenja
Nisam uvjeren/a	Nisem prepričan	Nisem prepričan v celoti	Nisem prepričan v celoti	Nisem prepričan v celoti	Nisem prepričan v celoti	Nisam uvjeren/a u potpunosti
Možda	Mogoče	Nisem prepričan deloma	Mogoče	Mogoče	Mogoče	Možda
Ne znam	Ne vem	Niti prepričan niti nisem prepričen	Ne vem	Ne vem	Ne vem	Ne znam
Prilično	Dokaj	Prepričan - deloma	Deloma prepričan	Deloma prepričan	Deloma prepričan	Djelomično sam uvjeren/a
Potpuno	Popolnoma	repričan - popolnoma	Popolnoma preprčan	Popolnoma preprčan	Popolnoma preprčan	U potpunosti sam uvjeren/a
Da će vam netko ukrasti službene podatke sa službenog računala (u firmi ili na fakultetu).	Da vam bo nekdo ukradel službene podatke iz službenega računalnika (v podjetju ali na fakulteti).	Da vam bo nekdo ukradel službene podatke s službenega računalnika (v organizaciji, kjer delate).	Da vam bo nekdo ukradel službene podatke iz službenega računalnika (v službi).	Da vam bo nekdo ukradel službene podatke s službenega računalnika (v organizaciji, kjer delate).	Da vam bo nekdo ukradel službene podatke s službenega računalnika (v organizaciji, kjer delate).	Da će vam netko ukrasti službene podatke sa službenog računala (u organizaciji u kojoj radite).
Da će vam netko ukrasti privatne podatke s vašeg kućnog računala.	Da vam bo nekdo ukradel privatne/osebne podatke s vašega osebnega računalnika.	Da vam bo nekdo ukradel podatke z domačega osebnega računalnika.	Da vam bo nekdo ukradel podatke z osebnega računalnika.	Da vam bo nekdo ukradel podatke z osebnega računalnika.	Da vam bo nekdo ukradel podatke z osebnega računalnika.	Da će vam netko ukrasti podatke s mobilnog telefona.
Da će vam netko ukrasti privatne podatke s vašeg mobilnog uređaja.	Da vam bo nekdo ukradel privatne/osebne podatke z vašega mobilnega telefona.	Da vam bo nekdo ukradel zasebne podatke z vaše mobilne naprave.	Da vam bo nekdo ukradel podatke z mobilnega telefona.	Da vam bo nekdo ukradel podatke z mobilnega telefona.	Da vam bo nekdo ukradel podatke z mobilnega telefona.	Da će vam netko ukrasti podatke s mobilnog telefona.
Da će vam netko otuđiti novac s vašeg računa u banci.	Da vam bo nekdo odujil denar z vašega bančnega računa.	Da vam bo nekdo vzel denar z vašega tekočega računa.	Da vam bo nekdo odtujil denar z vašega tekočega računa.	Da vam bo nekdo odtujil denar z vašega tekočega računa.	Da vam bo nekdo odtujil denar z vašega tekočega računa.	Da će vam netko otuđiti novac s vašeg tekućeg računa.
Da će vam netko ukrasti identitet na internetu (e-banking, Facebook, mail).	Da vam bo nekdo ukradel identiteto na internetu (e-banka, Facebook, mail).	Da vam bo nekdo ukradel vašo identiteto na iternetu (npr. E-bančništvo, Facebook, mail).	Da vam bo nekdo ukradel vašo identiteto na svetovnem spletu (e-banka, Facebook, elektronska pošta).	Da vam bo nekdo ukradel vašo identiteto na svetovnem spletu (e-banka, Facebook, elektronska pošta).	Da vam bo nekdo ukradel vašo identiteto na svetovnem spletu (e-banka, Facebook, elektronska pošta).	Da će vam netko ukrasti identitet na internetu (e-banka, Facebook, elektronska pošta).
Molimo vas da pažljivo pročitate opis pojedinih situacija te da u odgovarajući stupac ispod stupnja važnosti	Prosim vas da pozorno preberete opis posameznih situacij in da v odgovarjajoči stolpec pod stopnjo varnsti označite koliko	Prosimo vas, da pozorno preberete opis posameznih situacij ter da v pripadajoči stolpec odogovrite, koliko je po	Prosimo vas, da pozorno preberete navedene tditve, po vašem nenju ocenite koliko je pomembno izvajati	Prosimo vas, da pozorno preberete navedene tditve, ter ocenite koliko je pomembno izvajati zapisane	Prosimo vas, da pozorno preberete navedene tditve, ter ocenite koliko je pomembno izvajati zapisane	Molimo vas da pažljivo pročitate navedene tvrdnje i procijenite koliko je važno izvoditi napisane

označite koliko je prema vašem mišljenju važno raditi sljedeće stvari.	je po vašem mišljenju pomembno delati naštete stvari.	vašem mnenju pomebno delati naslednje stvari.	predstavljene aktivnosti in to označite v stolpcu, ki to izaža.	aktivnosti in to označite v stolpcu, ki to izaža.	aktivnosti. Pomembnost označite v stolpcu, ki to izaža.	aktivnosti te označite u odgovarajućem stupcu
Prema vašem mišljenju koliko je važno	Po vašem mnenju, koliko je pomembno	Koliko je po vašem mnenju pomembno?	Po vašem mnenju koliko je to pomembno	Koliko je po vašem mnenju pomembno?	Koliko je po vašem mnenju pomembno?	Koliko je po vašem mišljenju važno?
Stupanj važnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stopnja pomembnosti	Stupanj važnosti
Potpuno nevažno	Popolnoma nepomembno	Popolnoma nepomembno	Popolnoma nepomembno	Popolnoma nepomembno	Popolnoma nepomembno	Potpuno nevažno
Prilično nevažno	Povsem nepomembno	Deloma nepomembno	Deloma nepomembno	Deloma nepomembno	Deloma nepomembno	Djelomično nevažno
Ne znam	Ne vem	Niti pomembno niti nepomombno	Ne vem	Ne vem	Ne vem	Ne znam
Prilično važno	Deloma pomembn	Deloma pomembno	Deloma pomembno	Deloma pomembno	Deloma pomembno	Djelomično važno
Izrazito važno	Zelo pomembno	Zelo (popolnoma) pomembno	Zelo pomembno	Zelo pomembno	Zelo pomembno	Izrazito važno
Kopirati važnije dokumente na još jednu, drugu lokaciju odnosno drugi memorijski uređaj (izrada pričuvnih kopija podataka).	Kopirati pomembne dokumente na še eno drugo lokacijo oziroma drugi spominsko opremo (izdelava rezervnih kopij podatkov).	Kopirati pomembne dokumente še na eno drugo lokacijo oziroma na drugo spominsko enoto (izdelava varnostnih kopij podatkov).	Shranjevati pomembne dokumente še na eni lokaciji ali spominski enoti (oblikovanje kopij pomenbnih podatkov).	Shraniti pomembne dokumente še na eno lokacijo ali spominsko enoto (izdelava varnostnih kopij podatkov)	Shraniti pomembne dokumente še na dodatno lokacijo ali spominsko enoto (izdelava varnostnih kopij podatkov.	Pohraniti važne dokumente na još jednu lokaciju ili memorisjku jedinicu (izrada sigurnosnih kopija podataka).
Provjeriti tuđi usb memorijski štapić od virusa prije učitavanja podataka.	Preveriti tuji usb ključek zaradi virusov pred nalaganjem podatko.	Preveriti je tuj usb disk (usb ključ) okužen z virusi pred pregledovanjem podatkov.	Pred uporabo tujih usb medijev za prenos podatkovnih baz, preveriti ali so okuženi z virusi.	Pred uporabo tujega usb medija preveriti ali jr okužen z virusi, pred pregledovanjem podatkov.	Pred uporabo (pred pregledovanjem podatkov) tujega usb medija preveriti ali je okužen z virusi.	Prije učitavanja podataka s tuđeg usb medija, provjeriti je li zaražen virusom.
Bezuvjetno čuvati tajnost svojih zaporki.	Brezpogojno varovati tajnost svojih gesel.	Brezpogojno varovati tajnost svojih gesel.	Brezpogojno varovanje svojih gesel.	Brezpogojno varovanje svojih gesel.	Brezpogojno varovanje svojih gesel.	Bezuvjetno zaštiti svoje zaporke.
Periodično zamijeniti svoje zaporke novima, barem za važnije sustave.	Periodično zamenjati svoja gesla z novimi, vsaj za pomembnejše sisteme.	Periodično zamenjati svoja gesla, vsaj za pomembnejše sisteme.	Za pomembneješe sisteme pogosto menjavanje vstopna gesla.	Periodično zamenjati gesla za pomembneješe sisteme.	Periodična zamenjava gesel za pomembneješe sistem.	Povremeno mijenjati zaporke za najvažnije sustave.
Odvajati poslovne računalne resurse od privatnih (npr. Prijenosna memorija, elektronička pošta, telefon).	Ločiti poslovne računalniške vire od osebnih (prenosni disk, elektroska pošta, telefon).	Ločiti poslovne računalniške resurse od zasebnih (npr. Prenosni disk, elektronska pošta, telefon).	Ločiti poslovne vire od osebnih (npr. Prenosni disk, elektronska pošta, telefon).	Ločiti poslovne računalniške vire od osebnih (prenosni disk, elektroska pošta, telefon).	Ločiti poslovne računalniške vire od osebnih (prenosni disk, elektroska pošta, telefon.	Odvojiti poslovne računalne resurse od osobnih (prijenosni diks, elektronska pošta, telefon).
Čuvati od krađe svoj usb memorijski štapić sa važnim podacima.	Varovati pred krajo svoj usb ključek s pomembnimi podatki.	Varovati od kraje svoje usb disk (usb ključ) s pomembnimi podatki.	Pred krajo dobro zaščititi usb medij s pomembnimi podatki.	Varovati od kraje svoje usb disk (usb ključ) s pomembnimi podatki.	Varovati od kraje svoje usb disk (usb ključ) s pomembnimi podatki.	Čuvati od krađe svoj usb s važnim podacima.

PRVOTNA OBLIKA - ELEMENT	PREVOD 1	PREVOD 2	PREVOD 3	SKUPNI PREVOD	KONČNA VERZIJA	BACKTRANSLATION
Molimo vas da pažljivo pročitate opis pojedinih situacija te da u stupac ispod sigurnost osobnih podataka procijenite vašu situaciju.	Prosimo vas, da pozorn preberete opis posameznih situacij in da v odgovarjajoči stolpec pod varsnost osebnih podatkov osebitevašo situacijo.	Prosimo, da pozorno preberete opis posameznih situacij ter da v pripadajoči stolpec (pod varnost osebnih podatkov) ocenite vašo situaciju.	Prosimo vas, da pozorno preberete trditve in v stolpec označite v kolikšni meri veljajo za vas.	Prosimo vas, da pozorno preberete trditve in v stolpec označite v kolikšni meri veljajo za vas.	Prosimo vas, da pozorno preberete trditve in v stolpec označite v kolikšni meri trditve veljajo za vas.	Molimo vas da pažljivo pročitate tvrdnje i u stupac označite u kolikoj mjeri vrijede za vas
Sigurnost osobnih podataka	Varnost osebnih podatkov	Sigurnost osobnih podataka	Varnost osebnih podatkov	Varnost osebnih podatkov	Varnost osebnih podatkov	Sigurnost osobnih podataka
Nikada	Nikoli	Nikoli	Nikoli	Nikoli	Nikoli	Nikada
Ne sjećam se	Se ne spomnem	Ne spomnim se	Ne spomnim se	Ne spomnim se	Ne spomnim se	Ne sjećam se
U zadnjih 6 mjeseci	V zadnjih 6 mesecih	V zadnjih 6 mesecih	V zadnjih 6 mesecih	V zadnjih 6 mesecih	V zadnjih 6 mesecih	U zadnjih 6 mjeseci
U prošlih mjesec dana	Prejšnji mesec	V zadnjih mesec dni	V zadnjih mesec dni	V zadnjih mesec dni	V zadnjih mesec dni	U zadnjih mjesec dana
Prošli tjedan	Prejšni teden	Prejšji teden	Prejšji teden	Prejšji teden	Prejšji teden	Prošli tjedan
Kada steposljednji puta radili sigurnosnu kopiju (engl. Backup) osobnih podataka i dokumenata?	Kdaj ste zadnjič naredili varnostno kopijo (ang. Backup) osebnih podatkov in dokumentov?	Kdaj ste zadnji naredili varnostno kopijo vaših dokumentov (angl. "backup")	Kdaj ste zadnjič naredili varnostno kopijo (ang. Backup) osebnih podatkov ali dokumentov?	Kdaj ste zadnjič naredili varnostno kopijo (ang. Backup) osebnih podatkov ali dokumentov?	Kdaj ste zadnjič naredili varnostno kopijo (ang. Backup) osebnih podatkov ali dokumentov?	Kada ste posljednji put napravili sigurnosnu kopiju (eng. Backup) osobnih podataka ili dokumenata?
Koliko oseb pozna geslo za pristop v vašo elektronsko pošto?	Koliko oseb pozna geslo za pristop v vašo elektronsko pošto?	Koliko oseb pozna geslo za pristop v vašo elektronsko pošto?	Koliko oseb pozna geslo za vstop na stran vaše elektronske pošte.	Koliko oseb pozna geslo za pristop v vašo elektronsko pošto?	Koliko oseb pozna geslo za pristop v vašo elektronsko pošto?	Koliko osoba zna zaporku za pristup vašoj elektronskoj pošti
Više od 10	Več kot 10	Več kot 10	Več kot 10	Več kot 10	Več kot 10	Više od 10
Više od 5	Več kot 5	Več kot 5	Več kot 5	Več kot 5	Več kot 5	Više od 5
Ja i još 2 osobe	Jaz in še 2 osebi	Jaz in še 2 osebe	Jaz in še 2 osebe	Jaz in še 2 osebi	Jaz in še 2 osebi	Ja i još dvije osobe
Ja i još jedna osoba	Jaz in še ena oseba	Jaz in še ena oseba	Jaz in še ena oseba	Jaz in še ena oseba	Jaz in še 2 osebi	Ja i još jedna osoba
Samo ja	Samo jaz	Samo jaz	Samo jaz	Samo jaz	Samo jaz	Samo ja